Le jardin des plaisirs

Phil Caldero
11,5k abonnés 1600 vidéos

Tuto du catalogue des vidéos de la chaîne (le jardin des plaisirs) (12'40')

So long, Wayne Shorter ! (8'11' ') Vancouver-Piano Solo (6'12' ') Rules (3'03' ') Reckoner-piano solo (6'22' ') Stayin' alive (Cover by Rewind) (4'13' ') Honeysuckle Rose (Fats Waller) (2'03' ') Crystal Silence (Chick Corea) (4'41' ') Paranoid Android (Radiohead) (7'22' ') Célestin (piano solo) (4'24' ') Lady Madonna- Beatles cover on piano solo (4'27' ') Here comes the sun (The Beatles) (7'54' ') Let it ride-piano solo (6'34' ') The Preacher- Horace Silver (Piano solo) (4'37' ') Dans la peau de John le Pianiste (5'39' ') Keith Jarrett: Köln Concert / Sun Bear (Kyoto)-Cover (5'33' ') In a Silent Way (Tribute to Miles) Piano Solo Fantasy (Earth, Wind and Fire cover) Piano solo Everything in its right place (Radiohead cover) Piano solo"Self-evidence" Tribute for the 60th anniversary of the March on Washington (4'12' ')La Fiesta (Chick Corea Cover) Piano soloChildren (Alex Tassel cover) Piano Solo + sounds of children playingThe National Anthem (Radiohead cover) Piano solo The Mandelbrot Symphony Une brève histoire du Métal Ecclesiastes: Free my heart (Me'Shell Ndegeocello cover) Piano solo So Beautiful (Piano Solo- Robert Glasper cover-Feat Hugh Grant-Julia Roberts) Blue Velvet-Mulholland Drive (Lynch-Badalamenti on piano solo)

Mathématiques, agrégation, master et, surtout, du plaisir, du plaisir et du plaisir...

Table des matières

1 Les écrits (504)

1.1 Un peu de lecture (12)

1.1.1 Carnet de Voyage en Algébrie : la présentation

La seconde édition de carnet de voyage en Algébrie vient d'arriver chez Calvage & Mounet avec son lot de nouveautés que l'on présente ici.

1.1.2 Carnet de Voyage en Analystan : la présentation

La dernière version de carnet de voyage en Analystan vient d'arriver avec son lot de nouveautés que l'on présente ici.

1.1.3 Algèbre éclectique de Danila - Eiden - Mneimné - 1

Quelques mots (sans rentrer dans les détails) sur ce livre d'algèbre éclectique (niveau master) qui vient de paraître pour notre plus grand bonheur !

1.1.4 Algèbre éclectique de Danila - Eiden - Mneimné - 2

On ouvre le livre et on pioche dedans comme dans une boîte de chocolats.

1.1.5 Algèbre éclectique de Danila - Eiden - Mneimné - 3

On étudie les idéaux premiers de l'anneau (intègre) $\mathbb{Z}[X]/(X^4+1)$. Cela va nous permettre d'affiner nos outils pour les anneaux non principaux et se familiariser avec des morphismes qui nous ramènent gentiment à des anneaux principaux assez proches (comme $Q[X]$, Z, $\mathbb{F}_p[X]$)

1.1.6 Algèbre éclectique de Danila - Eiden - Mneimné - 4

Voici une petite équation matricielle, extraite du livre « Algèbre éclectique » de Danila-Eiden-Mneimné, faisant intervenir un polynôme irréductible sur Q. Vous ne verrez plus jamais de la même manière le petit théorème de l'existence des bases !

1.1.7 « Le groupe symétrique S_4 et ses métamorphoses » 1

Lecture d'été du joli livre d'Alain Debreil et Rached Mneimné chez Calvage et Mounet. Un livre qui ouvre toutes les fenêtres du groupe S_4 sur divers domaines des mathématiques. $Dix-sept$ chapitres, et autant de notes fleuries qui embaumeront cette fin d'été.

1.1.8 « Le groupe symétrique S_4 et ses métamorphoses » 2

On feuillette ici le livre des métamorphoses du groupe symétrique S_4.

1.1.9 « Le groupe symétrique S_4 et ses métamorphoses » 3

On continue à feuilleter chapitre par chapitre les pages du livre d'Alain Debreil et Rached Mneimné sur les nombreux avatars du groupe S_4 en géométrie affine, euclidienne, avec les polytopes, les graphes de Cayley, les treillis d'extensions de corps et enfin la géométrie projective. Ces deux derniers méritent un traitement à part qui figurera dans des vidéos prochaines.

1.1.10 « Le groupe symétrique S_4 et ses métamorphoses » 4

Le livre d'Alain Debreil et Rached Mneimné propose dans le chapitre II une série d'exercices d'un type nouveau. On veut savoir, si l'on se donne une permutation de S_4, de combien de manières peut-on décomposer cette permutation en un produit de 4-cycles, resp. 3-cycles, resp. d'un trois-cycle et d'une double-transposition. On donne une formule qui permet de calculer ce nombre dans un cadre très général : dans S_n, on fournit le nombre de décompositions en produit de m permutations appartenant chacune à une classe de conjugaison donnée. On montre cette formule dans une prochaine vidéo, et on se content d'exposer et d'illustrer cette formule, qui exploite la théorie des caractères.

1.1.11 « Le groupe symétrique S_4 et ses métamorphoses » 5

On prouve le résultat annoncé sur le nombre de décomposition dans S_n en types donnés. Cela demande de la théorie des caractères (lemme de Schur et surtout l'utilisation classique de la représentation régulière comme fonction caractéristique de l'élément neutre).

1.1.12 « Introduction aux graphes aléatoires » par l'épreuve Mines-Pont 2024 (et le livre)

Je saute sur l'occasion de la (difficile) épreuve 2, Mines-Ponts 2024, pour parler du livre de Roger Mansuy « Introduction aux graphes aléatoires » chez Calvage et Mounet. On parlera dans cette vidéo de fonctions de seuil pour certaines propriétés. Je trouve cela fascinant de voir de si belles idées dans un problème aussi appliqué.

1.1.13 Les perles d'Indra par David Mumford (and al.)

Perles d'Indra- 1 L' univers est fracatal Dans la mythologie védique de l'Inde ancienne, Indra est le dieu des dieux et son collier est constitué de perles se reflétant les unes aux autres, jusqu'à l'infini, et au-delà. Cette représentation poétique de l'univers, Felix Klein en a rêvé. David Mumford, Caroline Series et David Wright l'ont fait ! Dans un livre chaudement recommandé : Indra's pearls- the vision of Felix Klein.

Perles d'Indra- 2-Les premières perles

Une petite mise en place pour entrer de plain pied dans l'univers d'Indra. Quelques prérequis très sommaires sur l'action des homographies sur l'ensemble des cercles (ou droites). Puis, on construit nos premières perles du collier ainsi que leurs reflets.

Perles d'Indra- 3-Ping-pong, graphe de Cayley et plein de jolies couleurs

On met en place le ping-pong entre a et b, ce qui donne lieu à de jolies images pleines de couleurs, qui peuvent également se voir à l'aide du graphe de Cayley d'un groupe libre à deux générateurs (y a plus de flèches, mais moins de couleurs). On donne un exemple simple d'homographies a et b qui vérifient les « règles du ping-pong ».

Perles d'Indra- 4-on commence à assembler les perles (désolé, le son est mauvais au début)

On veut maintenant que le collier de perles soit constitué de disques tangents entre eux. Cela demande déjà au départ que les quatres disques initiaux le soient. Mais cela ne suffit pas. On trouve alors une condition nécessaire : que les points de tangence soient globalement conservés par les homographies a et b. Cela va impliquer par symétrie cyclique que les points de tangence sont fixés par des commutateurs. On en profite pour un petit exercice de santé : montrer que si quatre cercles sont cypliquement tangents, alors les points de tangence sont cocyliques.

Perles d'Indra- 5-dernier cours avant la récré

On arrive enfin à axiomatiser notre collier d'Indra. Tout d'abord, de façon géométrique, avec la notion de commutateur parabolique, puis, de façon purement algébrique, avec la formule des traces de Markov. On rencontre au passage l'équation classique $x^2 + y^2 + z^2 - xyz = 0$.

Perles d'Indra- 6-Playtime !

Le dernier volet de ce « reader's digest » d'un des plus beaux livres que j'ai eu entre les mains. On va maintenant, jouer avec les paramètres, et même dérégler la machine afin de construire à l'envi de jolies des courbes fractales.

1.2 Propédeutique (33)

1.2.1 Cahier de vacances - Roger Mansuy - Théorie des ensembles

Vive les vacances et ses cahiers. Pour se remettre en forme, on fait un petit « vrai-faux » sur la théorie des ensembles. Vous pourrez trouver le cahier sur

`http://www.rogermansuy.fr/pdf/CahierVacances.pdf`

1.2.2 Cahier de vacances - Roger - Mansuy - Complexes

Quelques exercices sur les nombres complexes. Vous pourrez trouver le cahier sur `http://www.rogermansuy.fr/pdf/CahierVacances.pdf`

1.2.3 Cahier de vacances - Roger Mansuy - Suites

Vive les vacances et ses cahiers. Pour se remettre en forme, on fait un petit « vrai-faux » sur les suites.

1.2.4 Cahier de vacances - Roger - Mansuy - fonctions continues

Pour se remettre en forme, on fait un petit « vrai-faux » sur les fonctions continues.

1.2.5 Cahier de vacances - Roger - Mansuy - Polynômes

Fuyez la chaleur et mettez-vous au frais pour ce petit questionnaire sur les polynômes.

1.2.6 Cahier de vacances - Roger - Mansuy - Espaces vectoriels

Pour se remettre en forme, on fait un petit « vrai-faux » sur les espaces vectoriels.

1.2.7 Cahier de vacances - Roger - Mansuy - Applications linéaires

Quelques exercices sur les applications linéaires (et les endomorphismes).

1.2.8 Cahier de vacances - Roger - Mansuy - Dimension

Quelques exercices sur la dimension. V

1.2.9 Cahier de vacances - Roger - Mansuy - Matrices

Quelques exercices sur les matrices.

1.2.10 Cahier de vacances - Roger - Mansuy - Matrices-2

Quelques exercices sur les matrices.

1.2.11 Questionnaire Roger Mansuy - Ensembles et Applications

Le questionnaire Vrai-Faux de Roger Mansuy qui concerne les bases des mathématiques dites modernes : la théorie des ensembles et les applications. Pour les amateurs de patates !

1.2.12 Questionnaire Roger Mansuy - Structures algébriques

Questionnaire Vrai-Faux de Roger Mansuy sur les structures algébriques

1.2.13 Questionnaire Roger Mansuy - Arithmétique - 1

Questionnaire Vrai-Faux sur l'arithmétique

1.2.14 Questionnaire Roger Mansuy - Arithmétique - 2

Le second volet du questionnaire d'arithmétique de Roger Mansuy

1.2.15 Questionnaire Roger Mansuy - Groupe de permutations

Site de Roger Mansuy

1.2.16 questionnaire Roger Mansuy sur les polynômes

Un petit questionnaire de niveau licence sur les polynômes.

1.2.17 Questionnaire Roger Mansuy Espaces Vectoriels 1

Attention, l'été rouille les méninges ! Une petite couche de questionnaire Roger Mansuy de temps à autre permet de limiter les dégats.
et venez vérifier les réponses sur la chaîne.

1.2.18 Questionnaire Roger Mansuy sur les espaces euclidiens - 1

Demandez le catalogue $Automne - Hiver$:

1.2.19 Questionnaire Roger Mansuy sur les espaces euclidiens - 2

Demandez le catalogue $Automne - Hiver$:
et le site de Roger Mansuy

1.2.20 Questionnaire Roger Mansuy sur les matrices

Questionnaire Vrai-Faux de Roger Mansuy sur les matrices

1.2.21 Questionnaire Roger Mansuy sur les déterminants

Malgré l'apparente simplicité des questions, ce questionnaire pensé avec soin par Roger Mansuy permet d'intégrer en profondeur cette première partie du cours d'agrégation interne sur les déterminants.

1.2.22 Questionnaire Roger Mansuy sur la réduction-1

Une première partie du copieux questionnaire Vrai-Faux de Roger Mansuy qui concerne le coeur du programme d'agrégation en algèbre, j'ai nommé la réduction. Encore une fois, ce questionnaire est instructif car il permet de prendre du recul sur les bases du programme.

1.2.23 Questionnaire Roger Mansuy sur la réduction 2

Une seconde partie du copieux questionnaire Vrai-Faux de Roger Mansuy qui concerne le coeur du programme d'agrégation en algèbre, j'ai nommé la réduction.

1.2.24 Questionnaire Roger Mansuy sur la réduction-3

la dernière partie du copieux questionnaire Vrai-Faux de Roger Mansuy qui concerne la réduction..

1.2.25 Questionnaire Roger Mansuy sur les séries entières

Questionnaire Vrai-Faux de Roger Mansuy sur les séries entières

1.2.26 Questionnaire Roger Mansuy sur les séries

1.2.27 Questionnaire Roger Mansuy - Suites

Questionnaire Vrai-Faux de Roger Mansuy sur les suites.

1.2.28 Questionnaire Roger Mansuy sur la topologie

Questionnaire Vrai-Faux de Roger Mansuy sur la topologie

1.2.29 Propédeutique. Les nombres complexes (décomplexés) pour l'agrégation interne

Histoire de partir d'un bon pied, on passe en revue tout ce qui est utile de savoir sur les nombres complexes (constructions du corps des complexes, calcul complexe, équations en complexe, géométrie des complexes).

1.2.30 Petit recueil d'idées reçues - 1 - Espaces vectoriels

On présente ici un florilège d'assertions que les candidats à l'agrégation interne ou externe croient à tort. Chaque assertion fausse sera déminée, d'une part en la rapprochant de l'assertion juste la plus proche, et d'autre part en exhibant un contre - exemple. En espérant que ce soit utile ! On commence par un premier chapitre sur l'algèbre linéaire et les espaces vectoriels.

1.2.31 Petit recueil d'idées reçues - 2 - Réduction

On présente ici un florilège d'assertions que les candidats à l'agrégation interne ou externe croient à tort. Chaque assertion fausse sera déminée, d'une part en la rapprochant de l'assertion juste la plus proche, et d'autre part en exhibant un contre - exemple. En espérant que ce soit utile ! On continue avec un chapitre sur la réduction.

1.2.32 Petit recueil d'idées reçues - 3 - Polynômes - Groupes - Anneaux

On présente ici un florilège d'assertions que les candidats à l'agrégation interne ou externe croient à tort. Chaque assertion fausse sera déminée, d'une part en la rapprochant de l'assertion juste la plus proche, et d'autre part en exhibant un contre - exemple. En espérant que ce soit utile ! On continue avec un chapitre sur les anneaux de polynômes et les groupes.

1.2.33 Petit recueil d'idées reçues - 4 - Formes quadratiques

On présente ici un florilège d'assertions que les candidats à l'agrégation interne ou externe croient à tort. Chaque assertion fausse sera déminée, d'une part en la rapprochant de l'assertion juste la plus proche, et d'autre part en exhibant un contre - exemple. En espérant que ce soit utile ! On finit en beauté avec un chapitre sur les formes quadratiques.

1.3 Cours (102)

1.3.1 Cours d'algèbre linéaire

1.3.2 Cours sur les espaces vectoriels

On commence un cycle d'algèbre linéaire qui figure au coeur du programme d'algèbre de l'agrégation interne. ici, il sera question de la définition des espaces vectoriels.

L'algèbre linéaire est au coeur du programme de l'agrégation, interne comme externe. Il est prudent d'entre d'un bon pied dans le monde des espaces *vectoriels/*

Partie 1. Il sera question de la définition des espaces vectoriels.

Partie 2. On attaque les premières définitions dans les espaces vectoriels : parties libres, génératrices.

Partie 3. Lemme d'échange qui permet de prouver que toutes les bases d'un espace vectoriel de dimension finie ont même cardinal.

Partie 4. On montre l'existence de base dans un espace vectoriel de dimension finie à l'aide du théorème de la base incomplète. On commence à traiter les problème sur corps finis.

Partie 5. Le théorème de la base extraite, dont on va tirer une conséquence classique : une partie génératrice est une base si et seulement si elle a le bon nombre d'éléments : la dimension (finie).

Partie 6. On traite ici le cas des sous-espaces vectoriels. Leur définition, leur caractérisation. On termine sur le fait qu'un sous-espace vectoriel d'un espace vectoriel de dimension finie est lui-même de dimension finie.

Partie 7. L'application emblématique de la dimension : elle permet une inclusion réciproque. Il s'agit d'un théorème (en fait dans le cours, d'un corollaire) qu'il faudra tout le temps avoir à l'esprit lorsque l'on traite d'une égalité de sous-espaces vectoriels. On calcule ensuite un problème de dénombrement sur corps fini.

Partie 8. Deux opérations (addition et intersection) sur l'ensemble des sous-espaces vectoriels d'un espace de dimension finie (ou pas) E. On donne une caractérisation intrinsèque de ces opérations, puis, on prouve la formule de Grassmann qui met en relation les dimensions des sous-espaces considérés.

Partie 9. Applications de la formule de Grassmann et sommes directes de deux ou plusieurs sous-espaces, et quelques critère de sommes directes.

Partie 10. On généralise le critère sur les sommes directes de deux sous-espaces à plusieurs sous-espaces. Il faut particulièrement se méfier ici d'une généralisation hasardeuse. Pour finir, on calcule le nombre de sous-espaces supplémentaires à un sous-espace fixé (sur un corps fini).

Cours d'agrégation interne sur les applications linéaires

On définit les objets fondamentaux autour des applications linéaires (opérations sur les applications linéaires, noyau et image, théorème fondamental de l'algèbre linéaire, formule du rang. On en déduit ensuite en exercice quelques résultats de dénombrement.

Cours sur la dualité

Le dual est à la dualité ce que le conjoint est au couple. C'est dire si l'affaire est sérieuse ! On commencera donc par parler de ce que l'on appelle le dual et surtout de la dualité (en dimension finie). On exhibera un tableau qui va transformer un objet de l'algèbre linéaire en un objet « dual ». On définira ensuite la « base duale » en dimension finie, on écrit deux formules qui se révèleront très pratiques dans la suite, et on fournira un contre - exemple en dimension infinie, où la « famille duale » d'une base n'est pas une base (elle est en fait uniquement libre mais non génératrice).

On vient de voir les bases duales. Comment le changement de base duale dans E^* s'opère-t-il en fonction d'un changement de base fixé dans E ? On se rend compte que si l'on part d'une matrice de passage P dans l'espace, alors on obtient une matrice de passage Q dans l'espace duale qui se trouve être, en générale, différente de P (Q est l'inverse de la transposée de P). Mais si l'on dualise une fois de plus la base duale, on obtient une matrice de passage à nouveau égale à P. Ceci permet de voir qu'il y a un isomorphisme indépendant d'une base choisie entre un espace E et son bidual.

On donne deux applications de la dualité, une à la formule d'interpolation de Lagrange, et une autre à la formule de Taylor polynomiale. On montre que ces deux formules découlent d'une démarche standard impliquant la recherche de bases duales l'une de l'autre.

On discrétise la formule de Taylor pour obtenir une formule générale qui calcule la somme $P(0) + P(1) + ... + P(m)$ pour tout polynôme P. On ne se prive pas d'utiliser la dualité.

On étudie maintenant la dualité des sous-espaces vectoriels pour aboutir à la notion d'orthogonal d'un sous-espace (attention, cet orthogonal doit être vu dans le dual !). On donne la dimension de cet orthogonal, puis, on étudie la dualité des opérations sur les sous-espaces vectoriels.

On introduit les hyperplans comme l'orthogonal d'une droite. Si une droite est un sous-espace non nul ayant un minimum de degrés de liberté, un hyperplan peut être vu comme un sous-espace ayant un minimum de contraintes. On discute les sous-espaces comme intersections d'hyperplans, ce qui revient à obtenir un sous-espace par son équation cartésienne.

Dans cette vidéo, on présente la transposée d'une application linéaire. Même si au final, elle correspond à la banale transposée d'une matrice, cette notion abstraite de transposée d'application linéaire demande une certaine habileté dans le maniement. On prouve que la transposée fournit une bijection linéaire entre les espaces $L(E, F)$ et $L(F^*, E^*)$.

On montre ici que la transposée, qui envoie bijectivement l'espace $L\ (E,\ F)$ sur $L(F^*, E^*)$, envoie les injectifs sur les surjectifs et inversement, les noyaux sur les images. Ce qui nous permet d'achever le dictionnaire de la dualité que nous avions mis en introduction du cours 5.

On jongle ici avec le bidual pour montrer que la transposée est involutive. Mais si f est dans l'espace $L\ (E,\ F)$ des applications linéaires, la transposée de sa transposée est dans $L\ (E^{**},\ F^{**})$. Que signifie donc l'égalité entre deux éléments qui n'appartiennent pas au même ensemble ? On va essayer d'expliquer cette subtilité. Ceux qui ne sont pas sensibles au concept alambiqué de bidual pourront se contenter de constater que la transposée possède une version matricielle beaucoup plus pratique.

On fait le point sur des applications de la dualité dans le programme et les développements de de l'agreg (interne ou externe). On trouvera des applications aux polynômes, aux matrices, en analyse, topologie, et bien sûr dans le cadre des formes quadratiques.

Minicours sur les matrices

On introduit les matrices, comme objet de calcul au service des applications linéaires. Pour l'instant on observe les liens entre matrices et applications linéaires, mais en mettant l'accent sur le fait que ces liens dépendent de choix de bases. En même temps on définit les coordonnées (en colonne) des vecteurs dans une base, et en ligne des formes linéaires dans la base duale.

On discute des opérations sur les matrices, l'addition, la multiplication par un scalaire et la multiplication de deux matrices (multipliables), le tout, en lien avec ce que ces opérations informent sur des opérations dans le monde des applications linéaires.

On définit deux involutions sur les matrices, tout d'abord la transposée et ensuite l'inversion des matrices (carrées inversibles !). On regarde à quoi correspond ces deux inversions dans le monde des applications linéaires (ou des endomorphismes).

On présente ici les matrices de passage comme des matrices de l'application linéaire (en fait l'endomorphisme) identité avec pour base de départ la nouvelle base et pour base d'arrivée l'ancienne base. On montre que cette définition permet de retrouver très facilement toutes les formules sur les matrices de passage.

On discute et on prouve ici l'incontournable théorème du rang qui dit que deux matrices sont équivalentes si et seulement si elles ont même rang.

On finit en beauté en calculant le nombre de matrices de taille (m, n) de rang r sur un corps fini de cardinal q. On le fait par application systématique du lemme du Berger et en suivant la preuve du théorème du rang.

Déterminants

(1h52'17' ')

A travers les résultats successifs, on voit **comment le déterminant**, qui démarre comme un calcul un peu pataud sur une matrice carrée, **acquiert ses titres de noblesses**. Le but de cette playlist est de **fournir les clefs d'une leçon sur le déterminant, tout en préparant le prochain cours sur la réduction**. Ici, on montre **le théorème principal du déterminant en insistant sur l'unicité d'une fonction vérifiant des propriétés simples, plutôt que sur sa formule explicite**.

On prouve et on illustre **le théorème principal d'existence et d'unicité du déterminant**.

On a montré que **l'ensemble des applications de $\mathbf{M_n(K)}$ dans $\mathbf{K}$ qui sont, à la fois, n-linéaires et alternées sont toutes proportionnelles au déterminant (et réciproquement).** On montre plusieurs **conséquences pratiques et théoriques** de ce résultat : **déterminant des matrices triangulaires, triangulaires par blocs, invariance par transposition du déterminant**. Mais c'est, surtout, **la multiplicativité du déterminant** qui **aura des conséquences profondes sur la suite du cours d'algèbre linéaire**.

On observe les conséquences de **la multiplicativité du déterminant** : $\det(AB) = \det(A)\det(B)$. Ceci **implique la stabilité par conjugaison du déterminant mais aussi le fait que le déterminant est capable de déceler si un système forme ou non une base d'où son**

nom amplement mérité. Mieux, **l'invariance par conjugaison permet d'élever le rôle du déterminant : on peut définir le déterminant d'un endomorphisme indépendamment d'un choix de base**. Enfin, on définit **la notion de mineur** et on énonce **la formule qui donne explicitement l'inverse d'une matrice inversible en fonction de la transposée de la comatrice**. Elle sera prouvée dans la prochaine partie.

On attaque **la preuve de la formule explicite de l'inverse d'une matrice (inversible)**. On étudie ensuite **les systèmes de Cramer**.

Voici une preuve d'un résultat sur le déterminant qui aura de multiples (mais bénéfiques) conséquences**. Le rang d'une matrice (rectangulaire, soyons fous) est égal à la taille maximale d'un mineur non nul**. On illustre **le déterminant dans sa maîtrise des contraintes : il peut donner l'équation d'une droite, vectorielle, affine et même l'équation d'un cercle**. On pourrait continuer avec les coniques mais on s'arrêtera là.

Une petite partie presque simpliste sur **le déterminant comme forme volume**.

On va parler sans preuves de **généralisations des résultats classiques sur le déterminant**. Tout d'abord, **le développement par rapport à une colonne (ou une ligne) se généralise en développement de Laplace ou développement par rapport à une famille de colonnes** (je me souviens qu'en math sup, j'avais intuité ce résultat mais n'ayant pas le sens de l'effort à l'époque, la rencontre avec la preuve ne s'était pas faite). Mais **le résultat le plus important est la formule de Binet** (qui généralise la multiplicativité du déterminant lorsque l'on fait le produit de deux matrices rectangulaires). On parle ensuite (un peu trop pour certains et pas assez pour d'autres) de **l'importance de cette formule en théorie des représentations et en géométrie algébrique.**

Cours 7 agrégation interne : réduction polynômes d'endomorphisme 1

On commence un nouveau cours d'agrégation interne sur la réduction. Tout d'abord avec une partie motivation l'histoire de comprendre où l'on va à partir de ce que l'on sait déjà. On rappelle donc brièvement ce que l'on a fait avec les applications linéaires et leurs matrices, l'histoire de lancer le programme.

Cours 7 Agrégation interne : Réduction polynômes d'endomorphisme 2

On commence par définir les polynômes d'un endomorphisme u d'un espace vectoriel E. Ce ci est défini comme un morphisme d'algèbre allant de l'agébre de polynômes $\mathbb{K}[X]$ vers l'algèbre des endomorphismes de E. Ce morphisme définit, d'une part, l'algèbre des polynômes de l'endomorphisme u, et d'autre part, le polynôme minimal de u, vu comme générateur de l'idéal noyau.

Cours 7 agreg interne : réduction polynômes d'endomorphisme 3

On attaque la preuve du lemme des noyaux, qui peut être vu comme un avatar de l'identité de Bezout (et finalement l'arithmétique des polynômes) dans la géométrie de l'espace E « muni de l'endomorphisme u ».

Cours 7 agreg interne : réduction polynôme d'endomorphisme 4

En mathématiques, on est toujours confronté au choix de la théorie et de la pratique. Le polynôme minimal est un polynôme annulateur (d'un endomorphisme u), plutôt du côté de la théorie. En revanche, le polynôme caractéristique est un polynôme plus facilement calculable par sa définition et également annulateur par Cayley-Hamilton. Ses racines sont les valeurs propres de l'endomorphisme u.

Cours 7 agreg interne : réduction polynômes d'endomorphisme 5

On prouve ici le théorème de Cayley-Hamilton par les matrices compagnon

Cours 7 agreg interne-externe : Réduction polynômes d'endomorphismes 6

On fait le point sur les propriétés du polynôme caractéristique. Degré, indépendance du corps, divisibilité par le polynôme minimal μ et divise μ^n.

Cours 7 agreg interne-externe : réduction polynôme d'endomorphisme 7

On a montré que le polynôme caractéristique était « coincé » entre le polynôme minimal et une puissance (égale à la dimension de l'espace) du polynôme minimal. On en donne une preuve alternative instructive lorsque le corps est le corps des complexes (ou un corps algébriquement clos). On en déduit ensuite le polynôme minimal et caractéristique d'un endomorphisme restreint aux sous-espaces caractéristiques.

Minicours sur les polynômes

La théorie des polynômes est intéressante en soi, mais avant tout, elle constitue un outil incontournable en algèbre linéaire (ainsi qu'en analyse). Voici un mini-cours où nous allons visiter les divers aspects de la théorie : définition, évaluation, division euclidienne, idéaux principaux, quotients ainsi que des aspects plus éloignés de l'arithmétique comme les racines, et les relations coefficients-racines. On fera également un détour du côté du résultant.

Cours 9 agreg interne : réduction diagonalisation 1

Voici la suite du cours sur la réduction. On étudie les matrices dites diagonalisables et on donne tous les critères classiques de diagonalisabilité, allant des critères géométriques aux critères, plus efficaces, qui impliquent les polynômes.

Cours 9 agreg interne : réduction diagonalisation 2

On présente les grands classiques des applications des critères polynomiaux de la diagonalisabilité. 1) l'induit d'un diagonalisable à un sous-espace stable est encore diagonalisable, 2) la diagonalisation simultanée, 3) diagonalisabilité des endomorphismes de multiplication par une matrice.

Cours 9 agreg interne : réduction diagonalisation 3

On tente ici de définir des fonctions « inverses » sur les matrices, comme la racine k-ième, le logarithme... On se rend compte que même si ces fonctions existent bien sur $\mathbb{C}$, elles ne sont pas forcément définissables sur $\mathcal{M}_n(\mathbb{C})$. La diagonalisabilité nous permet de le faire à l'aide de polynômes interpolateurs de Lagrange. Dans le cas non diagonalisable, on s'en sort sur un ouvert, en utilisant la décomposition de Dunford et en remplaçant astuceieusement les séries de Taylor par des polynômes en une matrice nilpotente.

Cours 9 agreg interne : réduction trigonalisation 1

On donne l'analogue des critères de diagonalisation dans le cadre de la trigonalisation sur un corps K. On a bien entendu le critère par le polynôme caractéristique scindé sur K, mais aussi un critère plus fort par l'existence d'un polynôme annulateur scindé. Enfin, un critère, géométrique est le bienvenu. Il se fera par l'existence d'un drapeau complet stable.

Cours 9 agreg interne : réduction trigonalisation 2

On donne des raffinements et des applications à la trigonalisation. Tout d'abord, le critère du polynôme annulateur scindé, et comme application la trigonalisation simultanée d'endomorphismes trigonalisables qui commutent. Nous passons ensuite à une jolie application qui peut être vue comme un « Cayley-Hamilton à plusieurs variables ».

Cours 9 agreg interne : réduction trigonalisation 3

On ouvre un volet sur les applications de la trigonalisation et de la trigonalisation simultanée (pour deux matrices trigonalisables qui commutent). On montre que le spectre du la puissance est la puissance du spectre, et que l'on a les mêmes commutations du langage avec l'exponentielle... On montre ensuite une version plus fine de la trigonalisation : si A est une matrice trigonalisable, elle est semblable à une matrice diagonale par blocs triangulaire à spectre singleton. La taille d'un bloc associé à une valeur propre est la multiplicité algébrique de la valeur propre. C'est la porte ouverte sur la décomposition de Dunford.

Cours 10 agreg interne : réduction et formes normales

On présente différentes formes normales pour les classes de similitudes. Formes diagonales, formes diagonales par blocs de Jordan, formes par matrices de compagnon. Ce qui caractérise une « forme normale » est sa simplicité, mais surtout l'unicité d'un élément de cette forme dans une classe. On résout ensuite un exercice de dénombrement des classes de similitude sur corps fini qui illustre notre propos.

Cours 10 agreg interne : réduction et invariants de similitude 1

On a collecté suffisamment de résultats généraux pour comment une série d'exercices à thème. On commence ici avec le thème des matrices semblables On va donc passer par ce que l'on appelle les invariants de similitudes. Mais, contrairement au cas des matrices équivalentes où tout était résolu avec le rang, les choses ne sont pas simples... On peut tout de même voir dans certains cas que deux matrices ne sont pas semblables, mais on mesure en même temps la faiblesse de nos critères. Patience...

Cours 10 agreg interne : réduction et invariants de similitude 2

On commence avec un exercice qui permet de faire un petit tour du domaine en matière d'invariants de similitude pour déterminer si deux matrices sont semblables ou non. On fait ensuite le point sur les invariants partiels (polynôme caractéristiques, minimaux et autres), et les invariants totaux (dimension des noyaux emboîtés) qui permettent d'analyser la situation.

Equations matricielles à l'agrégation

On va commencer une petite série sur les équations matricielles, vue comme une application classique de la réduction. On veut résoudre sur un exemple (qui se généralise facilement) d'équation de type $Q(X) = 0$, où Q est un polynôme scindé simple sur un corps $\mathbb{K}$ et X une matrice de $\mathcal{M}_n(K)$. On voit que l'ensemble des solutions est une réunion de classes de similitude, que l'on cherche à caractériser par leurs formes normales. On pose ensuite le même problème dans le cas Q scindé, amis non simple, ce qui nous oblige à faire appel aux réduites de Jordan. En appendice, on montre comment calculer le nombre de classes de similitude de l'ensemble solution en faisant appel aux séries génératrices.

Après avoir résolu une équation matricielle basée sur un polynôme annulateur scindé, on attaque le plus délicat problème d'un polynôme non scindé. Pour simplifier, nous travaillons dans $\mathbb{R}$. Les méthodes précédentes nous ont permis de résoudre le problème dans $\mathbb{C}$, mais comment obtenir les solutions sur $\mathbb{R}$? Le résultat repose sur une propriété essentielle de la réduction : deux matrices réelles $\mathbb{C}$-semblables sont $\mathbb{R}$-semblables. On a le même résultat en remplaçant $(\mathbb{R}, \mathbb{C})$ par $(\mathbb{K}, \mathbb{L})$ où $\mathbb{L}$ est une extension de $\mathbb{K}$.

On montre ici quelques techniques (non exhaustives) pour trouver les racines k-ièmes d'une matrice B, lorsque cela est possible. On se ramène grâce au lemme des noyaux au cas où le spectre de B est singleton. Si B est nilpotente, il n'y a pas toujours de solution, mais si B est inversible, on trouve toujours une solution à l'aide d'un lemme qui permet de relever le développement de Taylor de $(1+x)^{1/k}$ en 0 en une expression polynomiale. On finit ce volet concernant les équations matricielles en indiquant à qui veut bien l'entendre, le bon cadre pour le problème : la théorie des représentations de carquois.

On revient sur ce petit lemme qui permet de passer d'un développement de Taylor, sur $\mathbb{R}$, à une formule analogue au niveau matriciel. On va même un peu plus loin, si on sait que l'exponentielle fournit une bijection de l'ensemble des matrices nilpotentes sur les matrices unipotentes, on obtient que des jolies formules d'inversion sur les matrices (racines k-ièmes, logarithmes).

Minicours sur la topologie en algèbre linéaire

On essaie de motiver les troupes autour de l'utilisation de la topologie en algèbre linéaire et plus particulière ment dans le cadre de la réduction. Au menu : normes, équivalence des normes, topologie normique, quelques contre - exemples, les exemples d'utilisation (un florilège) et quelques critères de convergence de suites géométriques de matrices.

Minicours sur les formes quadratiques - 1/2

Les formes quadratiques exposées pour un cours d'agrégation interne (et externe si on généralise à un corps de caractéristique différente de 2).

On va trouver dans un premier temps toutes les premières définitions et toutes les connexions entre formes quadratiques, formes bilinéaires symétriques, matrices symétriques et changement de base.

On étudie l'orthogonalité pour une forme bilinéaire symétrique (dans le cas où celle-ci est non dégénéré, ce qui demande une petite définition préalable). On se rend compte que les choses ne cadrent pas tout à fait avec l'intuition que l'on se fait de l'orthogonalité : certains sous-espaces ne sont pas en somme directe avec leur orthogonaux. On a alors besoin d'un critère pour assurer que tout se passe bien.

Minicours sur les formes quadratiques - 2/2

Voici la seconde partie du cours d'agrégation sur les formes quadratiques.

Nous cherchons dans un premier temps les formes quadratiques telles que tout sous-espace possède un orthogonal en somme directe. Sur $\mathbb{R}$, on tombe naturellement sur la notion de forme quadratique définie. On fournit plusieurs critères, de natures différentes, pour qu'une forme quadratique soit définie positive.

On introduit ensuite, avec les motivations qui s'imposent, la notion d'adjoint d'un endomorphisme.

Puis, on attaque ici le gros morceau du cours (et ce ne sera pas le seul !) : le théorème de Sylvester. On va insister lourdement sur le fait qu'il se décompose en deux parties : existence et unicité de la signature ! La preuve utilisée pour l'existence se fait sur le critère d'orthogonal en somme directe que nous avions rencontré précédemment, et pour l'unicité, on utilisera la dimension maximale d'un sous-espace défini positif.

On présente ici le théorème spectral comme conséquence directe du théorème d'orthogonalisation simultanée. Cela fournit un développement agréable que l'on peut trouver dans Carnet de Voyage en Algébrie.

Cours 12 agreg interne : matrices hermitiennes 1

Voici un premier volet sur les formes hermitiennes. On suppose connus les résultats analogues sur les formes bilinéaires symétriques (congruence, Sylvester, théorème spectral) et on donne le résultat équivalent dans le cas hermitien.

Cours 12 agreg interne : matrices hermitiennes 2

On introduit, dans le cadre d'un espace hermitien, la notion d'adjoint d'un endomorphisme. On montre en préambule l'existence et l'unicité d'un tel adjoint, puis, que dans une base orthonormée (ou unitaire), la matrice de l'adjoint est la trans-conjuguée de la matrice de l'endomorphisme de départ. On prouve ensuite le théorème des endomorphismes normaux qui stipule qu'un endomorphisme est diagonalisable en base orthonormé si et seulement si il commute avec son adjoint.

Cours 12 agreg interne : matrices hermitiennes 3

On donne des exemples célèbres de matrices normales : matrices hermitiennes, antihermitiennes, unitaires et leur équivalents réels. On fait ensuite le point sur la façon dont les matrices hermitiennes et antihermitiennes généralisent la partie réelle et imaginaire...

Géométrie affine - le minimum vital à l'interne

Un beamer pour présenter le minimum à savoir sur la géométrie affine aux écrits de l'agrégation. Au menu :

Cours 13 agreg interne : Géométrie affine 1

Voici une introduction à la géométrie affine dans le cadre de l'agrégation. On commence par s'acclimater, voire, se rassurer, avec une mise en relation entre les objets de la géométrie affine et leurs homologues en géométrie vectorielle.

Cours 13 agreg interne : Géométrie affine 2

L'axiomatisation de la géométrie affine est plutôt simple, mais on peut l'aborder de deux manières. Une première axiomatisation « d'autorité », consiste à définir une application qui a un bipoint associe un vecteur, puis une définition des transformations affines. Mais on lui préférera la définition par les actions simplements transitives d'un espace vectoriel. Dans ce cadre, les notations et surtout, la définition des transformations affines, sont plus naturelles.

Cours 13 agreg interne : Géométrie affine 3

Pour comprendre l'affine, on fait référence à nos connaissances du vectoriel, et ce via la bijection (qui, à v, associe $A + v$) que l'on obtient entre un espace vectoriel et un espace affine associé. Maintenant, pour comprendre une application affine f, il est pratique d'avoir un point A invariant, c'est-à-dire tel que $f(A) = A$, car on pourra identifier ainsi f à un endomorphisme phi de l'espace. Or, l'existence d'un point invariant est lié à la réduction (1 est-il dans le spectre de phi ?). Nous voilà revenu dans notre domaine de connaissance !

Cours 13 agreg interne : Géométrie affine 4

On vient de voir que si l'endomorphisme associé ϕ à une application affine f ne voit pas 1 parmi son spectre, alors f possède un unique point invariant. Si on note A ce point invariant, la bijection b entre l'espace vectoriel E et l'espace affine muni du point A vérifie $f = b \circ \phi \circ b^{-1}$, et donc, finalement, on peut assimiler f et ϕ, ce qui est bien agréable. Malheureusement, on va devoir étudier les isométries qui on souvent 1 parmi leur spectre. Il va donc falloir composer des applications affines avec invariant avec des translations. On commence donc par une digression sur la loi rond et surtout, sa représentation matricielle en affine.

Cours 13 agreg interne : Géométrie affine 5

On prouve le théorème principal de ce cours : le théorème de décomposition réduite qui donne une condition générale pour qu'une application affine se décomposition unique en une translation (vérifiant certaines hypothèses) et une application affine à point fixe. Ce théorème est la clef pour passer de problèmes affines au monde plus domestiqué de la réduction des endomorphismes.

Cours 14 agreg interne : Géométrie affine euclidienne 1

On attaque la géométrie affine euclidienne. Après les petites définitions d'usage, on montre qu'une application de l'espace affine dans lui-même qui laisse invariante la distance euclidienne est nécessairement une application affine. Afin d'étudier ces applications, dites isométries affines, nous allons commencer par montrer que leur endomorphismes associés, c'est-à-dire les isométries vectorielles, vérifient la propriété demandées pour obtenir la décomposition réduite.

Cours 14 agreg interne : Géométrie affine euclidienne 2

On va classifier les isométries affines du plan euclidien. On commence bien entendu par les isométries vectorielles, en mettant l'accent sur l'étude de la valeur propre 1.

Cours 14 agreg interne : Géométrie affine euclidienne 3

On attaque maintenant la classification en dimension 3. Au programme, symétries glissées et vissages qu'il est bon de connaître. Un rapide coup d'oeil à la dimension n nous convaincra que la classification n'est pas beaucoup plus difficile !

Cours 14 agreg interne : Géométrie affine, barycentres et convexité 1

Voici un point de vue fécond sur la géométrie affine. On définit la notion de barycentre d'une famille finie de points, et les propriétés d'usage (homogénéïté, associativité). On travaille sur le corps des réels et on définit un ensemble convexe comme un ensemble stable par barycentres positifs, ce qui revient à dire, stable par segments. On montre qu'une application de l'espace affine dans lui-même est une application affine si et seulement si elle respecte la notion de barycentre. Ce théorème prouve que la convexité est bien au coeur de la notion d'espace affine (réel).

Cours 14 agreg interne : Géométrie affine, barycentres et convexité 2

On définit les points extrémaux E_X d'une partie convexe X de l'espace affine (réel). On montre que si g est un élément du groupe affine tel que $g(X) = X$, alors $g(E_X) = E_X$. Ceci va nous aider à comprendre les groupes d'isométries.

1.3.3 Addendum

Le principe du minmax

Comment les formes quadratiques voient les valeurs propres de leur matrice symétrique associée (dans une BON) ?

Partie I. Le théorème spectral assure qu'une matrice symétrique réelle S est diagonalisable en base orthonormée. On va donner une caractérisation de ses valeurs propres à l'aide de la forme quadratique que S définit naturellement sur $\mathbb{R}^n$ par $q(x) = (x, \mathrm{Sx})$. C'est le principe du minmax appelé également théorème de Rayleigh.

Partie II. Après deux petits exercices sur le sujet, afin de se mettre en jambes, on attaque la preuve du théorème complet appelé aussi théorème de Rayleigh. On trouve la preuve dans Nouvelles Histoires hédonistes de Groupes et de Géométries Chapitre V-D.27.

Partie III. (Plus pour l'agreg externe que l'interne) On termine cette série de vidéos sur le théorème de Rayleigh (minimax), en prouvant les inégalités de Weyl et le théorème d'entrelacement de Cauchy.

Prépa Ecrits : Formes quadratiques 1/8

Une série d'exercices sur les formes quadratiques pour préparer les écrits de l'agrégation. Le théorème d'Apollonius est un théorème classique sur des propriétés métriques du triangle. Ce premier exercice en donne une formulation moderne. Attention, à la fin, il y a une erreur de calcul, il faut lire $OA^2 + OB^2 + OC^2 = 3OI^2 + 2/3AJ^2 + 1/2BC^2$ (au lieu de $OA^2 + OB^2 + OC^2 = 4/3OI^2 + 2/3AJ^2 + 1/2BC^2$)

Prépa Ecrits. Formes quadratiques 2/8

Un autre exercice sur les formes quadratiques réelles (ou pas). Il permet de montrer comment déjouer le piège fréquent des formes non « définies positives » de la restriction dégénérée. On n'a plus des orthogonaux en somme directe. On sort alors le remède miracle du « gonflement hyperbolique ».

Prépa Ecrits. Formes quadratiques 3/8

On va se servir du gonflement hyperbolique dans un cas simple : Soit E un espace réel muni d'une forme quadratique non dégénérée q, on veut montrer que le groupe des isométries de q agit transitivement sur l'ensemble des vecteurs isotropes non nuls de E. Comment faisait-on pour montrer que O_n agit transitivement sur la sphère, on prenait un élément de norme 1 et on le compétait en une base orthonormée. Là, c'est pareil, sauf qu'il n'y a pas de base orthonormée.

Prépa Ecrits. Formes quadratiques 4/8

On présente progressivement le principe de Rayleigh ou principe du min-max en petite dimension. Il s'agit d'un caractérisation géométrique des valeurs propres. On en donne une application amusante sur une fonction trigonométrique.

Prépa Ecrits : Formes quadratiques 5/8

On veut montrer qu'en « écrasant » une sphère de façon linéaire sur un plan, on tombe sur l'intérieur d'une ellipse, et l'on voudrait aussi relier les éléments caractéristiques de l'ellipse avec la transformation linéaire. Encore une fois, le théorème spectral agit de façon magistrale sur les éléments.

Prépa Ecrit : Formes quadratiques 6/8

On attaque en deux vidéos la reconnaissance d'une conique à partir de son équation. On peut juger des coniques non dégénérées à partir de la donnée de deux données : une signature en dimension 2 et un déterminant de taille 3. Cette première vidéo permet d'éliminer les cas dégénérés.

Prépa Ecrits : Formes quadratiques 7/8

On donne un tableau qui permet une classification affine des coniques à partir de leur équation algébrique. Cette classification se fait grâce au théorème de Sylvester et à partir des trois mineurs principaux associés à la forme quadratique homogénéïsée provenant de l'équation de départ.

Prépa Ecrits. Formes quadratiques 8/8

On connaissait un lien fort entre formes quadratiques et réduction avec le théorème spectral. En voici un autre en arithmétique qui permet de voir si deux matrices de $\mathcal{M}_2(\mathbb{Z})$ sont $\mathbb{Z}$-semblables en leur associant des formes quadratiques. La $\mathbb{Z}$-similitude s'interprète alors sous forme de congruence des formes quadratiques.

Questionnaire sur les formes quadratiques pour l'agrégation

Pas description, tout est dans la vidéo.

Agrégation externe et interne : sous-espaces stables 1

On propose de travailler sur les sous-espaces stables par un endomorphisme. Il s'agit d'un problème où l'on perd pied rapidement. Mais on va commencer en douceur avec quelques petites définitions, deux questions fondamentales qui vont le fil rouge de la playlist, et quelques exemples à bien avoir en tête.

Agrégation externe et interne : sous-espaces stables 2

On attaque les problèmes de sous-espaces stables en lien avec le polynôme caractéristique. Celui-ci est irréductible sur $\mathbb{K}$ si et seulement les seuls sous-espaces stables sont triviaux. On montre ensuite que ceci est un cas particulier du cas de l'endomorphisme cyclique. Dans ce cas, les sous-espaces stables sont en bijection avec les diviseurs unitaires du polynôme caractéristique. Cela provient d'une jolie propriété de correspondance biunivoque entre sous-espaces stables pour la matrice compagnon C_P et idéaux de $K[X]/(P)$. On étudie ensuite des exemples où il y a un maximum, ou un minimum de sous-espaces stables.

Agrégation externe et interne : sous-espaces stables 3

Après une vidéo 2 contenant des résultats un peu tumultueux, on retrouve des eaux plus calmes avec des petits exemples classiques à bien connaître de sous-espaces stables possédant un sous-espace supplémentaire stable. Endomorphismes auto-adjoints, normaux, diagonalisables, et pour finir, lemme de Fitting et sous-espaces caractéristiques.

Agrégation externe et interne : sous-espaces stables 4

On a donné sous-espace u-stable facile à construire : le sous-espace stable par u, engendré par un élément x. On donne une condition simple sur x pour que ce sous-espace stable admette un supplémentaire u-stable : que son polynôme minimal local soit égal au polynôme minimal de u. On montre ensuite comment construire de tels éléments. On obtient alors un boulevard vers le théorème de décomposition de Frobenius.

Agrégation externe et interne : sous-espaces stables 5

On fait le point sur le théorème de décomposition de Frobenius sur quelques exemples, puis, on présente le théorème de semi-simplicité, c'est-à-dire que l'on trouve un critère polynomial pour qu'un endomorphisme vérifie que tout sous-espace stable possède un supplémentaire stable. Ce critère porte sur le polynôme minimal de u.

Agrégation externe et interne : sous-espaces stables 6

On finit le volet sur les sous-espaces stables en donnant quelques indications sur la façon de décrire tous les sous-espaces stables d'un endomorphisme.

Minicours sur le résultant

On définit le résultant, en insistant sur l'application linéaire dont il est issu que sur l'expression du déterminant qui le définit habituellement. On se propose dans les vidéos qui suivent de donner rapidement un pannel d'applications. Pour commencer, on calcule le discriminant du polynôme $X^3 + pX + q$.

On donne une propriété générale du résultant qui sera la clef des suivantes : le résultant se décline sur les anneaux et est compatible avec les morphismes d'anneaux (dans un sens à préciser). On en déduit deux conséquences importantes. La première dit que si deux polynômes unitaires sur $\mathbb{Z}$ sont premiers entre eux, ils restent premiers entre eux modulo p premier sauf pour un nombre fini de p. La seconde dit que l'ensemble des entiers algébriques est un anneau (c'est-à-dire stable par l'addition et la multiplication).

On attaque les applications du résultant en géométrie algébrique : intersections de courbes planes, équations cartésiennes d'une courbe rationnelle... et on finit avec une surprise.

1.3.4 Cours arithmétique

Premier cours d'arithmétique à l'agrégation interne

On introduit l'arithmétique, sans se voiler la face !

1. On commence donc un premier volet introductif, où on montre des techniques de résolution d'équations diophantiennes (*i. e.* dans l'anneau des entiers). Il sera question d'équations linéaires sur $\mathbb{Z}$, où le lemme de Gauss joue un rôle décisif.

2. On résout ensuite des équations diophantiennes affines (degré 1). On se sert de la réduction modulo n, de l'algorithme d'Euclide qui permet de trouver des solutions particulières et enfin du lemme de Gauss pour la solution générale sans second membre. On finit avec une équation linéaire à trois variables, car il m'a semblé que deux variables ne donnait pas un aperçu suffisamment général de la situation.

3. On traite ici d'équations de degré 2 sur les entiers. Encore une fois, on constate l'importance du calcul modulaire, du lemme d'Euclide, lemme de Gauss, décomposition en irréductibles et théorèmes d'unicité dans les méthodes.

4. On attaque le cours d'arithmétique avec l'étude de l'anneau $\mathbb{Z}$. On suit une procédure que l'on retrouvera avec d'autres anneaux, comme par exemple l'anneau des polynômes $\mathbb{K}[X]$. On attaque les inversibles, puis la division euclidienne, et en fin la classification des idéaux. C'est un idéal principal et on en verra plus tard les implications.

5. On décrit l'ensemble des idéaux de $\mathbb{Z}$ comme un ensemble ordonné (par l'inclusion) et muni de deux opérations : l'addition et l'intersection. On montre que l'on a une bijection entre les idéaux de $\mathbb{Z}$ et les entiers naturels (car $\mathbb{Z}$ est principal). L'ordre « contient » des idéaux instaure alors un ordre sur les entiers naturel qui n'est autre que l'ordre « divise ». De plus, addition et intersection des idéaux fournit deux opérations sur les entiers naturels : respectivement le pgcd et le ppcm.

6. Ce qui est présenté ici est un déroulement ordonné à bien connaître en arithmétique. On montre le passage important qui va de la construction d'un pgcd dans un anneau principal (ici, l'anneau est celui des entiers, mais cela pourrait être n'importe quel anneau principal) *jusqu'au* théorème fondamental qui stipule que tout nombre peut être décomposé de façon unique en un produit de nombres premiers. Au passage, on glanera ça et là le lemme de Gauss et son avatar, le lemme d'Euclide.

7. On commence avec les premières conséquences du théorème fondamental de l'arithmétique, en particulier l'existence des p-valuations. On montre comment ces p-valuations permettent de donner un critère de divisibilité, puis des formules pour les pgcd et les ppcm. On finit sur un synopsis qui fait le point sur tous les volets théoriques de ce premier cours (copieux) en arithmétique.

8. On a commencé avec des équations diophantiennes, on finit avec d'autres équations qui utilisent le lemme de Gauss, l'identité de Bezout, les propriétés caractéristiques du pgcd et du ppcm. On cherche des solutions rationnelles à une équation polynomiale et on parle de systèmes de congruence.

Préparation à l'écrit. Arithmétique 1

On résout ici l'équation diophantienne $x^2 + y^2 - 29z^2 = 0$ en mettant l'accent sur la factorialité de l'anneau $\mathbb{Z}[i]$ des entiers de Gauss $\mathbb{Z}[i]$.

Prépa Ecrits. Arithmétique 2

On avait déjà vu dans une vidéo sur les « Structures quotient » que $x^2 + y^2 - 31z^2 = 0$ avait pour seule solution $(0,\ 0, 0)$. Ici, on le montre à la suite de la vidéo « Arithmétique 1 » comme application immédiate de la factorialité de l'anneau $\mathbb{Z}[i]$ des entiers de Gauss.

Prépa Ecrits. Arithmétique 3

On étudie la divisibilité de la suite des nombres de Fibonacci F_n par un nombre premier fixé p. On montre qu'il existe une fonction α telle que p divise F_n si et seulement $\alpha(p)$ divise n... Et nous voici embarqués dans de curieuses considérations de savoir si 5 est un carré modulo p. Pas si curieuses au final, si on sait que l'équation caractéristique de la suite récurrente qui définit les nombres de Fibonacci est $X^2 - X - 1$, de discriminant 5. Errata, à un moment je dis que $b^2 + ab - a^2 = (b + a/2)^2 - 5a^2$, alors que c'est $b^2 + ab - a^2 = (b + a/2)^2 - 5(a/2)^2$

Prépa Ecrits. Arithmétique 5

Voici un autre exercice sur le lemme chinois. Cette fois-ci on le retrouve dans une version matricielle. Ceci permet de calculer le nombre de matrices inversibles de taille d sur l'anneau $\mathbb{Z}/m\mathbb{Z}$.

Prépa écrits. Arithmétique 6

Dans la vidéo Arithmétique 3, on regardait le problème de connaître l'ensemble des entiers n tels que le nombre de Fibonacci F_n soit divisible par un entier premier p. On passe maintenant du nombre premier p à un nombre entier quelconque m. On tombe sur une fonction arithmétique α telle que m divise F_n si et seulement $\alpha(m)$ divise n.

Prépa écrits. Arithmetique 7

Toute petite vidéo que je n'ai pas pu intégrer dans la précédente... On récolte ce que l'on a semé dans la vidéo Arithmétique 6 : on donne tous les nombres n tels que F_n se termine par exactement k zéros dans son écriture décimale. On rappelle que l'on a construit une fonction α telle que m divise F_n si et seulement $\alpha(m)$ divise n. Pour connaître $\alpha(m)$, il suffit donc de connaître $\alpha(p^k)$ pour tout p^k de la décomposition en facteurs premiers de m. Et ceci est donné par une récurrence qui différencie les pas $p \geq 3$ et $p = 2$.

Prépa écrits. Arithmétique 8-teaser

Une petite légende sur la bataille d'Hastings nous servira de point de départ de l'équation de Pell-Fermat. Il s'agit d'une équation de type hyperbolique, et il va falloir se rappeler cette vidéo « structure de groupe sur une conique 2/9 » pour générer toute une famille de solutions à partir d'une seule.

Prépa écrits. Arithmétique 8

On présente ici l'équation de Pell-Fermat. Un résultat dit que, si d est un entier positif non carré, alors l'ensemble des solutions positives de l'équation diophantienne $x^2 - dy^2 = 1$ a une structure de groupe isomorphe à $\mathbb{Z}$. On montre ici, que cet ensemble est soit trivial, soit isomorphe à $\mathbb{Z}$.

Prépa écrits. Arithmétique 9

Un peu parce que l'on veut avoir le dernier mot avec l'équation de Pell-Fermat $x^2 - dy^2 = 1$, un peu pour la culture générale, mais aussi, pour la beauté de la chose, on va donner un mini-cours (en deux vidéos) sur les fractions continues. Ici, on montre que si x est un irrationnel, il possède une écriture sous forme de fraction continue et que celle-ci fournit une suite de rationnels qui tend vers x et, même approxime x de façon remarquable (on parle d'approximation quadratique).

Prépa écrits. Arithmétique 10

Certaines équations diophantiennes comme l'équation de Pell-Fermat posent des problèmes d'approximation d'un réel par un rationnel. Plus particulièrement, l'équation de Pell-Fermat pose le problème d'approche d'un nombre quadratique par un rationnel. Il est alors temps de montrer ce joli théorème de Lagrange qui dit qu'un réel est quadratique si et seulement si sa décomposition en fraction continue est périodique à partir d'un certain rang.

Prépa écrits. Arithmétique 11

On finit par montrer, à l'aide des fractions continues, que l'équation de Pell-Fermat $x^2 - dy^2 = 1$ possède des solutions non triviales ! Attention à la fin, « faute de frappe » $324 + 325 = 649$ au lieu de 349 !

Prépa écrits. Arithmétique 12

Comme prétexte à présenter le petit lemme de Hensel, qui vient souvent épauler le lemme chinois, on se donne comme objectif de trouver un majorant pour le nombre de matrices M vérifiant $M^m = C$ sur un corps quelconque, où C est la matrice compagnon d'un polynôme P tel que $P(0) \neq 0$. Attention, errata, la borne du nombre de racines est évidemment m^s et non pas ms comme annoncé !

Minicours sur les structures quotient pour l'agrégation interne

Les structures quotient constituent une difficulté majeure à l'agrégation interne. On essaie d'introduire ici la nécessité de ces structures en l'argumentant sur des exemples dans divers dommaines (ensembles, groupes, espaces vectoriels, réduction, anneaux, équations diophantiennes)

Préparation aux écrits. Gymnastique des corps 1

Dans la série de vidéos qui suit, il ne s'agira pas de théorie des corps, mais juste d'un exposé de survol des différents types de corps sur lesquels on travaille dans le contexte de l'écrit, et pour chacun de ces types (caractéristique, finitude, ordre, algébriquement clos, les spécificités du corps des réels...) quels sont ouvertures que nous offre ce type et quel sont les pièges. J'en parlerai dans le contexte 1) des algèbres de polynômes, 2) de la réduction 3) des formes quadratiques. Dans cette première vidéo, on regarde attentivement les conséquences et les pièges qui se présentent selon si le corps sur lequel on travaille est fini ou non.

Préparation aux écrits. Gymnastique des corps 2

Après avoir étudié le spécificités des corps infinis ou finis, on s'attaque au cas des corps de caractéristique zéro ou p.

Préparation aux écrits. Gymnastique des corps 3

Ici, on regarde ce qui est possible ou pas, selon si l'on travaille (sur des polynômes, en réduction, ou formes quadratiques) sur un corps algébriquement clos ou non. On regarde ensuite les problèmes de caractéristiques 2 (ou pas).

Préparation à l'écrit. Gymnastique des corps 5

On continue sur ce volet de la pratique des corps à l'écrit de l'agrégation. On attaque ici une série de quatre vidéos sur les changements de corps. Sur cette vidéo un peu bavarde, il sera question de voir que chez les corps, les problèmes se font dans deux directions : la montée (on va chercher dans un corps plus grand des racines, des valeurs propres, des décompositions de polynômes...), et la descente (on a obtenu des information sur le corps du dessus, et on veut en déduire des informations sur le corps du dessous). Pour la montée, il sera question de théorème de Steinitz, de corps de décomposition, et de rupture. Pour la descente, on donnera quelques aperçus pratiques de la théorie de Galois forcément sous-jacente, mais sans pour autant faire de la théorie de Galois.

Préparation à l'écrit. Gymnastique des corps 6

On attaque ici les problèmes de descente dans des cas pratiques. Tout d'abord, le pgcd de polynômes est invariant par changement de corps ; Puis, on voit que le rang d'une matrice possède également cette propriété d'invariance. C'est la porte ouverte à une première approche, sous forme d'exercices, de problème d'invariance par extension de corps invariants de classes de similitudes. On étudie le cas diagonalisable, nilpotent, et enfin la décomposition de Dunford.

Préparation à l'écrit. Gymnastique des corps 7

On pénètre ici le coeur du problème : montrer que deux matrices carrées sur un corps $\mathbb{K}$ sont semblables si et seulement si elles sont semblables sur une extension $\mathbb{L}$. Cette preuve se fait en deux temps : un premier temps où $\mathbb{K}$ contient toutes les valeurs propres et un second où il ne les contient pas. Dans ce dernier cas, on fait intervenir le corps de décomposition du polynôme caractéristique.

Préparation à l'écrit. Gymnastique des corps 8

On finit pour l'instant ce volet sur les extensions de corps et les théorèmes de descente. Autant ceux-ci fonctionnent trivialement pour la réduction, autant pour les formes quadratiques, on tombe sur des problèmes plus délicats, comme le prouve le théorème de Sylvester, qui est typiquement réel. On pourrait continuer longtemps sur ce sujet et peut-être le ferons-nous ultérieurement, par exemple, en parlant de semi-simplicité des endomorphismes, de la séparabilité, de théorèmes de descente en théorie des représentations... mais ces choses (passionnantes) sont un peu moins urgentes.

1.3.5 Addendum Arithmétique

Fonctions arithmétiques à l'agrégation

On est partis pour un tour d'horizon sur les fonctions arithmétiques que l'on rencontre à l'agrégation. On commence ici par la fonction indicatrice d'Euler et la fonction mu de Moebius.

On continue avec l'ubiquité de la fonction mu de Moebius dans différentes composantes des mathématiques, où elle joue un rôle d'inversion pour la convolution, théorie des corps, arithmétique, réduction, et enfin en analyse avec les séries où l'on rencontrera l'inévitable fonction zeta.

Minicours sur les réseaux aux écrits de l'agrégation

On aborde ici une étude de réseaux dans $\mathbb{Z}^n$. Ce n'est pas une théorie, mais plutôt une approche pragmatique pour comprendre comment ceux-ci interviennent dans les problèmes d'agrégation.

Avant de résoudre quelques questions clefs du problème d'agrégation interne 2012 (EP1), nous commençons par énoncer quelques résultats qui seront prouvé par la suite. Ces résultats sont exposés dans un tableau permettant de comparer le résultat sur $\mathbb{Z}$ (sous-groupe de $\mathbb{Z}^n$) avec son analogue sur un corps (sous-espaces vectoriels de K^n).

On explique ensuite le pourquoi et le comment des réseaux.

On continue l'étude des sous-groupes de $\mathbb{Z}^n$, en suivant en filigrane l'épreuve EP1 de l'agrégation interne 2012. On prouve l'existence de $\mathbb{Z}$-bases, après avoir prouvé l'unicité du cardinal de telles bases. On prouve ensuite que ces bases sont en bijection avec le groupe $\mathrm{GL}_n(Z)$. On montre alors notre maitrise parfaite de la situation dans le cas $n = 2$, où l'on s'aide de l'identité de Bezout.

Nous prenons ensuite un bon départ dans l'étude des sous-groupes de $\mathbb{Z}^n$ en prouvant l'existence d'un $\mathbb{Z}$-base pour tout sous-groupe G de $\mathbb{Z}^n$, et même une condition pour qu'un élément du sous-groupe G se complète en une $\mathbb{Z}$-base de G.

On va faire quelques prolongations avec une adaptation sur $\mathbb{Z}$ du théorème de la base incomplète. Pour cela, on en arrive à la notion de groupe « sans torsion ». On finit (sans preuve, et sans les main) avec le théorème de la base adaptée.

1.3.6 Cours sur les groupes

Minicours sur les groupes cycliques

Partie I. On introduit les groupes cycliques, d'une manière un peu grossière (comme groupe isomorphe à $\mathbb{Z}/n\mathbb{Z}$, puis, de manière plus abstraite (groupe fini monogène). On donne ensuite quelques exemples (et contre - exemple) de groupes cycliques dans la nature.

Partie II. Nous allons montrer une propriété d'hérédité des groupes cycliques : tout sous-groupe d'un groupe cyclique est lui-même cyclique. Mieux, pour tout diviseur de n, il existe un unique sous-groupe (cyclique) de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d. On exploite ensuite cette propriété pour établir une formule sur la fonction d'Euler, puis pour donner une caractérisation des groupes cycliques par le nombre de ses éléments d'ordre fixé.

Partie III. On déduit de la caractérisation des groupes cycliques par leur nombre d'éléments d'ordre fixé, que tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique. On illustre ceci avec la conjecture d'Artin sur les générateurs de $((\mathbb{Z}/p\mathbb{Z})^*, \times)$. On montre ensuite le rapport avec le nombres premiers dits « longs », c'est à dire les nombres premiers p tels que l'écriture décimale de $1/p$ est de période $p-1$.

Partie IV. On attaque le problème des actions de groupes cycliques. Dans un premier temps, on donne toutes les actions d'un groupe cyclique sur un ensemble fini n. Puis, on donne des exemple d'actions impliquées dans des théorèmes célèbres (lemme de Cauchy, loi de réciprocité quadratique, collier de perle). Ces actions sont juste évoquées, et non pas détaillées.

Minicours introduction aux actions de groupes par le dénombrement

Une petite introduction qui j'espère, vous convaincra de l'utilité très concrète des actions de groupes. On programme : lemme du berger et formule des classes. Mais surtout, beaucoup d'exemples concrets d'utilisation, dans le cadre de la combinatoire ainsi que la combinatoire algébrique.

Questionnaire Groupes : Action (ou vérité)

L' avantage d'une série de questions sur les actions de groupes, c'est qu $'en$ même temps qu'on s'entraîne groupes, on révise tout le programme d'algèbre ! Avec les groupes, jouez à plusieurs ! It's more fun to compete.

P. S. Merci à *N. P.* pour le titre

Agrégation externe. Minicours de théorie des représentations 1

Un mini-cours en théorie des représentations complexes de groupes finis. On commence par tenter sans outil préalable les représentations de petits groupes finis. Ce préambule est essentiel pour comprendre ensuite ce que l'on fera une fois la théorie assimilée.

Agrégation externe. Minicours de théorie des représentations 2

On continue avec l'étude « à la main » de la théorie des représentations. rien de tel que le système D pour forger un « caractère ». On passe au groupe $\mathbb{Z}/3\mathbb{Z}$ qui nous permet de comprendre ce qui se passe pour tout groupe cyclique, puis le premier groupe non abélien S_3.

Agrégation externe. Minicours de théorie des représentations 3

On définit les représentations, les morphismes de représentations, et on montre le théorème de Maschke.

Agrégation externe. Minicours de théorie des représentations 4

On s'attaque à la classification des représentations d'un groupe. Par Maschke, on voit qu'il suffit de trouver toutes les représentations irréductibles. Elles se trouvent toutes dans la représentation dite régulière du groupe, qui est un cas particulier de représentation par permutation.

Agrégation externe. Minicours de théorie des représentations 5

On prouve ici le théorème d'orthonormalité des caractères avant d'en découvrir les multiples corollaires

Agrégation externe. Minicours de théorie des représentations 6

On donne ici les conséquences théoriques du résultat de Schur qui dit que les caractères irréductibles forment une base orthonormée de l'espace des fonctions centrales sur le groupe. On va voir que le caractère caractérise la représentation à isomorphisme près.

Agrégation externe. Minicours de théorie des représentations 7

Après avoir vu les conséquences théoriques du théorème de Schur sur la base unitaire des caractères, nous en découvrons les côtés pratiques avec tout un univers de petites recettes pratiques qui contribuent au bonheur et à l'harmonie dans la belle algèbre.

Agrégation externe. Minicours de théorie des représentation 8

Un préambule important avant d'attaquer la construction des tables de caractères : comment tirer parti d'une action de groupe pour en extraire un caractère irréductible qui figurera sur une ligne du tableau ?

Agrégation externe. Minicours de théorie des représentations 9

On commence à construire des tables de caractères. Pour se mettre en jambes : la table du groupe cyclique et celle du groupe symétrique S_3.

Agrégation externe. Minicours de théorie des représentations 10

La table de caractères du groupe S_4 a la taille parfaite être présentée en 15 minutes un jour d'oral. On va donc passer le temps qu'il faut pour l'étudier sous plusieurs aspects. Voici pour commencer une construction de la table de S_4 telle qu'elle se généralise à S_n (avec un peu plus d'effort, certes, mais l'idée, due à Frobenius, reste la même). Scoop : on n'utilise même pas la connaissance préalable de la signature qui, dans cette construction provient de la dualité dans les partitions.

Agrégation externe. Minicours de théorie des représentations 11

On commence à donner un sens plus empirique à toutes les représentations irréductibles de S_4. Action de groupes et tensorisation par la signature sont les mots clef.

Agrégation externe. Minicours de théorie des représentations 12

Cette fois on réinterprète la table de caractères de S_4 en termes géométriques. Pour cela, on réalise S_4 d'une part comme groupe d'isométrie du tétraèdre régulier, d'autre part comme groupe d'isométries positives du cube.

Minicours de théorie des représentations pour l'agrégation externe 13

On attaque une nouvelle série où l'on part de la table de caractères du groupe et où on en trouve des explications. Après un petit briefing sur le schéma général de ces applications dans divers domaines, on regarde sur des exemples où l'on calcule des multiplicités de représentations irréductibles dans une représentation donnée.

Minicours de théorie des représentations 14

On continue des exemples géométriques où il fait sens de décomposer une représentation en irréductibles. Un, avec les quadrilatères du plan, muni de l'action cyclique, et un autre, avec l'action des rotations du cube sur des faces.

Minicours de théorie des représentations 15

On prépare une petite extension du lemme de Schur dans le cas où la représentations n'est pas nécessairement irréductible mais seulement sans multiplicité. Cela va nous permettre par la suite (vidéos 16 et 17) de présenter de l'analyse harmonique discrète (mais non moins élégante !)

Minicours de théorie des représentations 16

On présente ici une version du théorème de Thébault par la théorie des représentations. La construction d'un carré à partir d'un parallélogramme peut se comprendre facilement si l'on voit cette construction comme un morphisme de représentations dont l'image est l'espace des carrés par une version modifiée du lemme de Schur vue dans la vidéo précédente. Le théorème de Napoléon est également discuté sous le même angle de l'analyse harmonique.

Minicours de théorie des représentations 17

On termine ce petit volet sur l'analyse harmonique avec l'exemple classique de A. A. Kirillov déjà présenté dans la vidéo 14. Il s'agit d'un exemple simple permettant d'indiquer comment la théorie des représentations s'est introduite dans la physique, liée aux transformations linéaires conservant une certaine structure.

Minicours de théorie des représentations 18

On attaque maintenant un nouveau volet sur ce que disent les tables de caractères de G sur le groupe fini G. Il se trouve que l'on va pourvoir retrouver tous les sous-groupes distingués de G. On regardera dans une prochaine vidéo des sous-groupes distingués particuliers comme le centre et le groupe dérivé.

Minicours. Théorie des représentations 19

On montre de façon pratique de façon théorique, puis sur des exemples, comment tirer le centre et le groupe dérivé de la table de caractères.

Minicours. Théorie des représentations. L'indicateur de Frobenius-Schur

Il se calcule avec la trace et il est capable de dire si la représentation se réalise sur un espace réel ou non. C'est ce joyau de la théorie des représentations que l'on a nommé l'indicateur de Frobenius-Schur !

Structure de groupe sur une conique-I

Voici une petite série de vidéos où l'on présente une construction de groupe sur les coniques. Il s'agit d'une construction qui fait le point sur des propriétés géométriques des coniques bien cônues depuis Pascal, et dont les applications à la cryptographie (que l'on effleurera seulement) sont apparues de façon relativement récente. Cette première vidéo est avant tout un teaser.

Dans cette vidéo, on donne la construction générale pour la structure de groupe sur une conique non dégénérée. On montre que l'on a bien un groupe dans trois cas particuliers. Et ces groupes ne sont pas anodins. Il s'agit du groupe additif (pour la parabole), du groupe multiplicatif (pour l'hyperbole), et le groupe additif modulaire, comme les groupe des angles, (pour l'ellipse). Si on ajoute à cela que ces groupes géométriques sont à la fondation de la cryptographie actuelle, on se dit qu'il n'y a que les maths pour nous faire traverser, dans une logique implacable, l'histoire antique, notre monde actuel, et les souvenirs nostalgiques des premières opérations de notre enfance.

Après avoir mis une opération sur une conique (munie d'un point), et après avoir montré que cette opération fournit une structure de groupe sur trois exemples représentatifs de la classification affine, on montre que la structure de groupe se transmet d'une conique à l'autre par une transformation affine. Et contre cette transmission, il n'y a ni masque, ni geste barrière !

Structure de groupe sur une conique-II

On attaque le théorème principal. Sur le fait que notre opération géométrique confère une structure de groupe qui caractérise le type affine de la conique. Au passage, on montre, à l'aide de changements de variables, le résultat souvent mal digéré sur la fameuse classification affine des coniques. Ce résultat sera parachevé dans une vidéo suivante.

On finit ici la preuve du théorème de classification des coniques non dégénérées par les trois groupes classiques réels.

On a montré le théorème de structure de groupe sur une conique, à l'aide d'un mélange de petit calculs dans trois cas simples et de groupes de transformations. On veut maintenant une preuve plus directe en travaillant sur la géométrie de la conique. L'associativité pose un petit problème, qui va être résolu grâce au théorème de l'hexagramme mystique de Pascal.

On a eu besoin d'une version projective du théorème de l'hexagramme mystique de Pascal. Voici quelques notions de projectif pour mieux comprendre ce que veut dire « envoyer une droite (ou un point) à l'infini » dans les manipulations de géométrie (projective). On verra également que le projectif confond paraboles, ellipses et hyperboles, alors que l'affine les distingue.

Structure de groupe sur une conique-III

On pensait arrêter là, mais l'arithmétique a mis le pied dans la porte, et on est repartis sur deux autres vidéos. Ici, on s'intéresse toujours à la structure de groupe sur une conique, mais cette fois-ci sous l'angle de l'équation diophantienne dite de Pell-Fermat. On verra trois groupes isomorphes : la conique de l'ensemble des solutions entières de l'équation, l'ensemble des unités positives d'un anneau quadratique réel, et tout bonnement, le groupe monogène des entiers.

Dernier volet de la série où l'on montre (en mode DSK) comment les coniques, en leur ajoutant une droite, sont des dégénérescences d'une famille de courbes elliptiques. On finit sur des explications (à détailler avec de bonnes références !) sur les applications de ces dernières à la cryptanalyse et à la cryptographie.

1.4 Thème-Algèbre linéaire (88)

1.4.1 Algèbre linéaire générale

Théorème de la base incomplète en version continue ?

Le théorème de la base incomplète est probablement le premier pas en algèbre linéaire. Sur un espace réel, il est naturel de se poser la question s'il possède une version continue, c'est-à-dire s'il existe par exemple une application continue qui envoie un vecteur non nul (ie libre) en une base qui le contient. Le résultat pourra en surprendre plus d'un.

1.4.2 Les délices de matrices

1 - Matrices d'applications linéaires

Critère par les mineurs pour le rang d'une matrice On montre ce résultat souvent utilisé : le rang d'une matrice rectangulaire est la taille maximale d'un mineur non nul. On en donne ensuite une application sur les corps $\mathbb{R}$ ou $\mathbb{C}$, à la topologie du rang (Nouvelles histoires hédonistes chapitre I)

Sous-espaces de matrices avec des conditions de rang-1 Une petite histoire soufflée par Rached Mneimné. On sait qu'un hyperplan de matrices carrées contient une matrice inversible. Et cela constitue un développement souvent présenté aux agrégations internes et externes. Mais a-t-on vraiment besoin d'un hyperplan ? Peut-on prendre une dimension plus petite ? On trouve ici une borne telle que si la dimension d'un sous-espace matriciel se trouve au-dessus de cette borne, alors il contient forcément une matrice inversible.

Sous-espaces de matrices avec des conditions de rang-2 On montre les résultats annoncés dans la vidéo 1. Finalement, un joli développement équilibré entre polynômes, propriétés du rang, déterminant, et on finit en beauté avec les corps finis (ou pas).

2 - Matrices et réduction

Réduction des matrices de rang 2 On part d'un exercice classique où l'on prouve qu'une matrice carrée de rang 1 est diagonalisable si et seulement si sa trace est non nulle. On donne ensuite des conditions de diagonalisibilité d'une matrice de rang 2 en fonction de sa trace et de la trace de son carré. Ceci ne sera pas sans rappeler le joli résultat de réduction (par congruence) de la forme quadratique qui, à une matrice M de taille n, associe le coefficient en X^{n-2} de son polynôme caractéristique.

Exercices de confinement Réduction 6 Voici quelques petits exercices de réduction autour des propriétés arithmétiques du polynôme minimal. On cherche ici le polynôme minimal d'une matrice diagonale, puis, triangulaire, par blocs.

Petit exercice ludique sur les matrices entières inversibles Cinq minutes sur un petit exercice étonnant de Patrice Lassère, qui fait intervenir des matrices à coefficients entiers.

Cayley + Hamilton = Lagrange ! Derrière cette égalité à peine exagérée se cache une connexion pas toujours connue des étudiants, entre la théorie des groupes finis abéliens (et même parfois par extension des groupes finis tout court) et la théorie de la réduction d'un endomorphisme sur un corps. C'était une réponse à une question naturelle de Titouan Martin !

(Non Riri, ce n'est pas un poisson d'avril ! : -)))

Cayley-Hamilton, la preuve 100% bio ! Voici résolument (!) ma preuve préférée du théorème de Cayley-Hamilton ! Avec que des bons produits ! Elle se dit uniquement en termes de structures et de morphismes, dans ce que l'algèbre moderne fait de plus élégant ! D'ailleurs, on va rapidement de rendre compte que l'on est sur une preuve bien plus forte que son propos de départ, et qui va nous propulser directement vers les fameux invariants de similitude (le Graal de la réduction).

Un scoop sur Cayley-Hamilton ? Tout étudiant ayant en main sa licence de mathématiques a forcément rencontré le théorème de Cayley-Hamilton, et son corollaire immédiat qui dit que le polynôme minimal d'une matrice divise son polynôme caractéristique. Mais qui sait ce que représente, en termes de matrices, le quotient du polynôme caractéristique par le polynôme minimal ? Et comment peut-on vivre dignement sans le savoir ?

Une preuve express de Cayley-Hamilton (sur tout corps et sans topologie) On présente une preuve très rapide de Cayley-Hamilton qui ne nécessite pas de topologie et ne demande pas d'hypothèse sur le corps. Elle demande en revanche la connaissance du discriminant d'un polynôme.

Exercices sur le thème « arithmétique au secours de la réduction » Deux exercices (plus une variante) où l'arithmétique des polynôme vient délivrer la réduction de ses problèmes de diagonalisabilité !

Décomposition de Dunford pour de « petits » polynômes minimaux Un exercice instructif sur la décomposition de Dunford qui utilise Bezout, la formule de Taylor polynomiale, Cayley-Hamilton, et un certain monsieur Newton (mais ça c'est un peu spoiler). Le but du jeu est ici de calculer explicitement la décomposition de Dunford d'une matrice à « petit » polynôme minimal. Petit... au sens de la divisibilité.

Disques de Gershgorin... et raffinements On présente ici une façon rapide de localiser les valeurs propres d'une matrice avec les disques de Gershgorin. On en donne une preuve élémentaire et on continue avec deux raffinements possibles : un par dualité, et un autre, plus impliqué, qui utilise la topologie des valeurs propres (voir vidéo précédente sur la continuité du spectre).

Diagonalisation et trigonalisation simultanées On présente les grands classiques des applications des critères polynomiaux de la diagonalisabilité. 1) l'induit d'un diagonalisable à un sous-espace stable est encore diagonalisable, 2) la diagonalisation simultanée, 3) diagonalisabilité des endomorphismes de multiplication par une matrice.

On présente ensuite des raffinements et des applications à la trigonalisation. Tout d'abord, le critère du polynôme annulateur scindé, et comme application la trigonalisation simultanée d'endomorphismes trigonalisables qui commutent. Nous passons ensuite à une jolie application qui peut être vue comme un « Cayley-Hamilton à plusieurs variables ».

Endomorphismes de l'espace des matrices qui commutent à la transposée Un petit exercice qui se décline bien selon si on se retrouve dans le contexte d'une leçon sur la dualité, de la diagonalisabilité, ou de la trigonalisabilité. Bref, un exercice, mais trois méthodes !

Un exercice classique sur le commutant On résout l'exercice classique que le commutant d'un endomorphisme est de dimension supérieure ou égale à celle de l'espace. On donne plusieurs preuves selon le niveau ou les affinités : une preuve algébrique, une preuve topologique et un qui provient de la combinatoire algébrique.

Tout sur le commutant (1ère partie) On propose de faire le point sur tous les résultats classiques à l'agrégation sur le commutant. Dans une première partie on étudie deux cas « complémentaires » que l'on retrouve souvent dans les écrits : le cas diagonalisable et le cas cyclique, ou si l'on préfère la matrice diagonale ou la matrice compagnon.

Tout sur le commutant (suite et fin) On propose de faire le point de tous les résultats classiques à l'agrégation sur le commutant. Dans une première partie on a étudié le cas diagonalisable et le cas cyclique. Cette fois-ci, on s'attaque au cas général, en nous basant sur le théorème de décomposition de Frobenius, plus particulièrement, les degrés des polynômes invariants de similitude.

Multiplication à gauche par une matrice- analyse spectrale Si A est une matrice carrée, la multiplication à gauche par A fournit un endomorphisme L_A de l'espace des matrices carrées (de même taille que A). On propose une analyse spectrale (spectre et vecteurs propres) lorsque A est diagonalisable. Bref, l'ambiance à son comble au Fab-Lab.

Une famille libre sur Q par la trace ! Un exercice qui peut parfaitement faire office de développement (corps, polynômes, dimension, déterminant...) propose de montre qu'une certaine famille finie de réels quadratiques sur $\mathbb{Q}$ est $\mathbb{Q}$-libre. Ceux qui n'en sont pas encore convaincus verront que la trace a de l'audace, la trace a du génie !

Qui sont les coefficients du polynôme caractéristique ? On prouve une formule générale pour les coefficients du polynôme caractéristique d'une matrice carrée A.

Sous-espaces de matrices stables par conjugaison On va trouver tous les sous-espaces de $\mathcal{M}_n(K)$ stables par conjugaison de $\mathrm{GL}_n(K)$. Evidemment, il sera question ici de réduction, mais aussi, curieusement, de décomposition en base 2, et on rencontrera également la jolie forme bilinéaire trace. On trouvera cet exercice dans le chapitre III de Nouvelles Histoires Hédonistes de Groupes et de Géométries.

Sous-espaces de matrices diagonalisables On discute ici de résultats sur les sous-espaces de $\mathcal{M}_n(K)$ constitués de matrices toutes diagonalisables.

Suites récurrentes linéaires (par la réduction) Inspirés par l'épreuve 1 de l'agrégation interne 2010, on propose une présentation des suites récurrentes linéaires à valeurs dans $\mathbb{C}$, via la réduction de l'endomorphisme de décalage (le shift S qui envoie u_n sur u_{n+1}). On y apprendra (peut-être) que l'ensemble des suites récurrentes linéaires est une $\mathbb{C}$-algèbre sur laquelle S agit de façon compatible avec les opérations. On s'amusera à réduire S et retrouver avec bonheur ses sous-espaces propres, et sous-espaces spectraux.

Un exercice sur les suites récurrentes linéaires et barycentres Voici un petit exercice proposé par Denis Roussillat sur le thème des suites récurrentes linéaires où l'on construit la suite à l'aide de barycentre. On donne ici deux versions de l'exercice, et deux solutions, une, élémentaire et l'autre niveau $M1$.

Comatrice, qui es-tu ? On cherche une définition intrinsèque (sans calcul et liée à l'algèbre linéaire plutôt qu'au calcul matriciel) de la comatrice. Il y a une définition savante qui utilise les algèbres extérieures, mais celles-ci sont hors programme agreg-master. On en propose une « intermédiaire » assez amusante.

Endomorphismes nilpotents à l'écrit de l'agreg (2017) On s'intéresse à la question $I6$) de l'écrit MG-2017 de l'agrégation externe. Il s'agit de classifier les classes de similitudes de certains endomorphismes nilpotents. Cela nous donne l'occasion de faire le point sur les techniques de réduction dans le cadre nilpotent. Deux mots d'ordres : suite des noyaux itérés et scindage de ces noyaux, voir Nouvelles histoires hédonistes de groupes et de géométries, chap. III.

Endomorphismes nilpotents à l'écrit de l'agreg-2 (variantes) Après avoir résolu cette question sur la classification des classes de matrices nilpotentes d'indice 2 en dimension 4, on tente quelques variantes (pour le plaisir). Quelles sont les classes de similitudes de matrices nilpotentes a) d'indice 2 en dimension nb) dont le noyau est de dimension $1c$) d'indice 3 en dimension 6.

La suite des noyaux emboîtés On explique dans un premier temps l'importance de la suite des noyaux emboîtés pour la classification des endomorphismes, en se ramenant aux nilpotents. Dans le cadre de l'étude des classes de similitude, la dimension des noyaux emboîtés est un invariant. On montre ici que cette suite est croissante, et qu'elle s'essouffle ! Pour finir, on indique sans preuve, pourquoi cette suite permet de déterminer exactement la classe de similitude de l'endormorphisme.

Le corps $\mathbb{C}$ est algébriquement clos (preuve par la réduction) On propose cette preuve du théorème de d'Alembert-Gauss ($\mathbb{C}$ est algébriquement clos), adapté d'une preuve de Pierre Samuel (provenant de celle de Legendre) dans le cadre de la réduction des endomorphismes. On peut trouver cette preuve dans Carnet de Voyage en Algébrie I-3.37.

Un exercice sur autour du théorème spectral (formule d'Apollonius) La formule d'Apollonius relie les distance entre les sommets d'un triangle et le milieu d'un côté. Le théorème spectral permet d'en voir une généralisation tous azimuths en dimension n.

Semblables sur $\mathbb{C}$ vs semblables sur $\mathbb{R}$ Deux matrices réelles sont semblables sur $\mathbb{C}$ si et seulement si elles sont semblables sur $\mathbb{R}$. On montre ce classique de la réduction. Mais on va un peu plus loin avec l'équivalence U_n -semblable/O_n semblables. Encore une application de la décomposition polaire.

Sous-espaces stables et polynômes minimaux Un petit exercice autour de ce thème. Au final une petite question piège (ou pas) est-ce qu'un sous-espace stable par u possède un supplémentaire stable si et seulement si le polynôme minimal de u est égal au ppcm du polynôme minimal de l'induit et celui du coinduit.

Un exercice instructif sur les matrices nilpotentes (avec un regard neuf sur la dérivation !) On propose un exercice qui trouvera sa place à un oral d'agrégation interne. On part d'une équation matricielle pour arriver à montrer qu'une des matrices en présence se doit d'être nilpotente. Mais cet exercice possède un intérêt en soi : il nous donne l'occasion d'aborder un peu la théorie de Lie...

Trace et nilpotence en toute caractéristique Un développement à l'agrégation consiste à prouver qu'une matrice A de taille n sur un corps de caractéristique nulle est nilpotente si et seulement si tr $(A^k) = 0$ pour tout k de 1 à n. Mais que devient ce critère en caractéristique quelconque ? Une question de Jean Parazuelo et une jolie remarque de Yann Dev en commentaires sur cette chaîne permette d'y répondre.

Lemme de Brauer sur les matrices de permutation Une nouveauté dans la dernière édition de Carnet de Voyage en Algébrie qui vient de sortir. On montre ici que deux permutations sont conjuguées dans le groupe S_n si et seulement si les matrices de permutation correspondantes sont conjuguées dans le groupe $\mathrm{GL}_n(K)$, c'est-à-dire semblable. Il s'agit d'un joli développement transversal où l'on va devoir récupérer des invariants de conjugaison dans S_n à partir d'invariants de similitude dans $\mathrm{GL}_n(K)$. Dans un premier temps, nous supposons que le corps $\mathbb{K}$ est de caractéristique nulle, et on pourra retrouver les invariants de conjugaison des permutations par la trace. Dans un deuxième temps, nous supposons que le corps $\mathbb{K}$ est de caractéristique quelconque, et une jolie matrice symétrique réelle va nous tirer d'affaire.

Sous-algèbres réduites de matrices complexes On commence par une question de jury autour de la décomposition de Dunford. Puis, on montre que si une sous-algèbre de $\mathcal{M}_n(\mathbb{C})$ ne possède pas de matrice nilpotente non nulle, alors, elle est conjuguée à une sous-algèbre de l'algèbre des matrices diagonales de $\mathcal{M}_n(\mathbb{C})$.

Sous-espace engendré par les matrices nilpotentes Quel est le sous-espace engendré par les matrices nilpotentes. Voici trois méthodes possibles : 1) une assez rapide sortie du chapeau, 2) une instructive pour l'agrégation, 3) une par un argument d'autorité qui nous emmènera vers les routes de la recherche !

Réduction par blocs-addendum On part d'une matrice A de taille n pour construire une matrice B de type anti-diagonale de taille $2n$ et dont les blocs diagonaux sont I_n et A. On donne dans cette vidéo tous les éléments de réduction de B en fonction de ceux de A. Après discussion en commentaire avec Toto, voici une approche "orthogonale" des classes de similitude par les dimensions de noyaux itérés.

Réduction par blocs avec une célèbre matrice On part d'une matrice A de taille n pour construire une matrice B de type anti-diagonale de taille $2n$ et dont les blocs diagonaux sont I_n et A. On donne dans cette vidéo tous les éléments de réduction de B en fonction de ceux de A.

Matrices semblables et tableaux de Young Comment montrer que deux matrices carrées complexes sont semblables ? On a vu dans une vidéo récente des petits contre-exemples classiques qui montraient que les invariants comme le polynôme caractéristique, minimal, le rang, et même tous ceux-là conjoints ne suffisaient pas pour conclure. A la suite d'un post de

Tom Fourgon sur cette chaîne, en prépa MP, je tente de montrer comment se servir de l'outil tableau de Young.

Polynômes diagonalisant (et autres polynômes liés à la réduction) Les polynômes diagonalisant portent bien leur nom : P est dit diagonalisant pour la matrice A si P(A) est diagonalisable... Mais qui sont-ils ?

Contre-exemples : matrices non semblables, alors que... Donner des exemples de matrices ayant même rang, même polynôme caractéristique, même polynôme minimal... alors qu'elle ne sont pas semblables. Voici le moment parfait pour réviser nos invariants de similitude !

Contre-exemples en réduction On propose ici une série de contre-exemples en réduction à savoir dégainer au bon moment ! Elles sont basées sur la notion de matrice compagnon dont nous expliquons rapidement quelques règles.

4 matrices symétriques non diagonalisables ! On me rapporte une question de jury : "citez-moi une matrice symétrique non diagonalisable". Voici 4 réponses possibles, dans 4 corps différents.

10 critères de diagonalisabilité ! (et leurs contre-exemples) Voici de quoi briller en société avec pas moins de dix critères qui vous donneront l'occasion de décider si une matrice est diagonalisable.... ou pas ! On passe de critères géométriques, ou des critères polynomiaux bien connus, pour passer à des critères structurels, topologiques, métriques... et des tellement hors-sol que l'on ne saurait les nommer :-)

Diagonalisable vs exp-diagonalisable !

On montre qu'une matrice complexe A est diagonalisable si et seulement si son exponentielle est diagonalisable. On en donne ensuite quelques applications dans des équations matricielles.

Un exercice sur l'exponentielle de matrices

Un exercice mais deux preuves pour cet exercice qui consiste à prouver que $(I+A/n)^n$ tend vers $exp(A)$ pour toute matrice carrée complexe. Et oui, le problème c'est qu'il nous faut ici, comme en complexe, une méthode qui n'utilise pas le logarithme ! I'm a Poor logarithmless cowboy !

Cas d'égalité entre trace et rang...

Une petite suite à l'exercice sur l'inégalité, bel exercice d'ailleurs avec rang, similitude, trace, formes quadratiques réelles... Il est naturel de poser la question fatale du cas d'égalité.

Un petit exercice sur trace et rang !

Voici un petit exercice tout chaud pondu du jour sur la trace et le rang... et un petit quelque chose de plus mais faut pas spoiler, c'est à vous de trouver.

Systèmes linéaires

Décomposition LU - Un survol rapide des choses à bien connaître La décomposition LU est à bien connaître, en particulier, pour l'oral de l'agrégation externe. Quelles sont les hypothèses ? Formuler l'unicité, prouver l'implication et sa réciproque, connaître les cas particuliers sur les corps classiques, et bien sûr savoir donner la complexité de l'algorithme ainsi que les extensions du domaine (Cholesky, décomposition PLU)

Pseudo-inverse d'une matrice réelle
On donne ici **l'expression de la pseudo-inverse d'une matrice**. Si Ax=b est un système linéaire et si B est la pseudo inverse de A, alors x=Bb est l'élément de norme minimale tel que (Ax -b) est de norme minimale.

Conditionnement d'une matrice
Parmi les applications des valeurs propres attendues dans la leçon 149 (selon le rapport du jury de l'externe), **on va trouver le conditionnement d'une matrice. Le conditionnement permet de comprendre la sensibilité des solutions trouvée à un système de Cramer Ax=b, en fonction des erreurs commises sur le calcul de la matrice A et du vecteur colonne b**. Pour la norme subordonnée à la norme quadratique, on trouve que le conditionnement est fortement lié à l'étendue du spectre de la matrice A*A.

Calcul d'une série exponentielle
On cherche à **calculer explicitement la série génératrice exponentielle d'un polynôme réel**. Un exercice qui demande un peu de calcul et également un peu de savoir-faire. En particulier, le choix d'une base adaptée de l'espace des polynômes et la résolution d'un système linéaire.

Solution optimale d'un système linéaire Voici (sous forme d'exercice) une façon élégante proposée par Moore et Penrose de formuler une solution optimale à un système linéaire quelconque sur $\mathbb{R}$. On aboutit à la notion de pseudo-inverse d'une matrice rectangulaire.

Matrices et norme euclidienne

Le théorème spectral (et ses avatars) On présente ici le théorème spectral comme conséquence directe du théorème d'orthogonalisation simultanée. Cela fournit un développement agréable que l'on peut trouver dans Carnet de Voyage en Algébrie.

Introduction aux matrices de Gram Une toute petite introduction aux matrices de Gram. Une définition dans le cas euclidien, quelques propriétés et surtout l'application classique au calcul de la distance d'un vecteur à un sous-espace. Pour finir, une résurgence de la matrice de Gram à un endroit où l'on ne s'y attend pas...

Le rang d'une matrice de Gram On montre ici que le rang de la matrice de Gram d'une famille de vecteurs de $\mathbb{R}^n$ est égal au rang de la famille. Ce sera l'occasion pour nous de parler de critère de rang par les mineurs et (accessoirement) de la dégéneresence d'une forme bilinéaire symétrique par restriction.

Gram-Schmidt et la décomposition QR On introduit ici la méthode d'orthonormalisation de Gram-Schmidt ainsi que son avatar matriciel : la décomposition QR. On présente ensuite l'avantage de cette décomposition (unicité, inégalité d'Hadamard...)

MG-2023-O_n-semblable vs GL_n-semblable-1 Dans la série « anatomie d'une épreuve d'agrégation », on va disséquer la partie IV du problème MG-2023 (ou peu s'en faut). On montre ici le résultat suivant : deux matrices symétriques sur $\mathbb{C}$ sont $\mathrm{GL}_n(\mathbb{C})$ -semblables si et seulement si elles sont $O_n(\mathbb{C})$ -semblables. On utilisera une « pseudécomposition polaire » sur $\mathbb{C}$, que nous démontrerons dans une prochaine vidéo.

MG-2023 - Partie IV-pseudo décomposition polaire sur un corps On présente ici ce qui semble une mine de petites techniques pour un candidat qui voudrait bien se préparer aux épreuves de l'écrit de l'agrégation. Il s'agit de montrer que sur le corps des complexes (puis sur un corps algébriquement clos de caractéristique différente de 2), toute matrice inversible se décompose en le produit d'une matrice orthogonale et d'une matrice symétrique.

Produits de matrices symétriques réelles Le produit de deux matrices symétriques est en général non symétriques. Mais, sur $\mathbb{R}$, si une des deux matrices est définie positive, alors la matrice produit est diagonalisable sur $\mathbb{R}$ et l'on peut même statuer sur le signe de ses valeurs propres. On en déduit une preuve alternative de l'unicité de la décomposition polaire.

Décomposition polaire

Décomposition polaire-Appellation controlée-1 Voici le premier volet d'une série consacrée à la décomposition polaire. Dans cette première partie, nous allons présenter la décomposition polaire, ses déclinaisons et autres avatars sur des groupes variés et ses cas dégénérés. On finit avec la décomposition polaire du groupe $O_n(\mathbb{C})$. Attention, contrairement à ce que l'on pourrait penser, il ne s'agit pas d'une n-ième développement sur la décomposition polaire, mais plutôt ce que l'agrégatif doit connaître lorsqu'il aborde le sujet.

Décomposition polaire-Dans tous ses états-2 Après avoir vu la décomposition polaire de divers sous-groupes de $\mathrm{GL}_n(R)$ ou $\mathrm{GL}_n(\mathbb{C})$, nous voici partis sur diverses interprétations de la décomposition polaire. Une interprétation géométrique pour commencer, puis une interprétation sur le thème optimisation des distances dans un espace normé, et pour finir en beauté avec une interprétation topologique de l'homéomorphisme de décomposition polaire.

Décomposition polaire- Applications-3 De la même manière qu'un théorème n'est rien sans ses corollaires, une décomposition de matrices n'est rien sans ses applications. La première des applications de la décomposition polaire est l'incontournable lien entre norme subordonnée à la norme quadratique et rayon spectral. Après avoir prouvé ce point on s'attaque à la maximalité du groupe orthogonal comme sous-groupe compact de $\mathrm{GL}_n(R)$. On continue avec des problèmes de connexité et de composantes connexes. On finit en beauté avec une application de la décomposition polaire à la forme volume.

La décomposition polaire vue par une ellipsoïde On propose ici de regarder la décomposition polaire sous un angle géométrique. On donne une preuve géométrique de l'existence, puis une interprétation géométrique de l'unicité de la décomposition.

Disques de Gershgorin, optimisation et inégalités.
On repasse rapidement en revue les disques de Gershgorin. On montre ensuite en quoi ces disques sont optimum pour localiser les valeurs propres (pour les amateurs de leçon 149 par exemple). On prouve ensuite deux inégalités déterminantales, une sur $\mathbb{C}$ et une autre, plus précise, sur $\mathbb{R}$.

Théorème spectral

Une nouvelle preuve du théorème spectral ? Une preuve nouvelle, et due à Clément de Seguins Pazzis, du théorème spectral, est tombée récemment sur les réseaux sociaux. C'est peut-être le moment de faire le point sur ce théorème et sur ses preuves.

Une nouvelle preuve du théorème spectral ? −2 Une jolie proposition de Hugues Contini pour une preuve du théorème spectral : en fait une propriété bien connue des polynômes irréductibles réels font que la seule obstruction au théorème spectral se situe en dimension 2. Le reste est une vérification de routine.

Théorème spectral (dernière preuve avant la rentrée) Voici une preuve très stylée du théorème spectral, proposée par Toto-toto. Il s'agit d'une preuve totalement algébrique (modulo $\mathbb{C}$ est algébriquement clos qui finalement ne est pas tant algébrique que ça malgré son pseudo « théorème fondamental de l'algèbre ») et qui n'utilise aucune récurrence (ça c'est juste pour l'exercice de style, on ne fait pas d'induction-bashing sur la chaîne !). Une preuve qui peut parfaitement figurer dans un cours d'agrégation interne.

Théorème spectral- une preuve totalement analytique ! Une preuve original du théorème spectral due à Yan Doumerc qui, dans un pur exercice de style, ne s'est autorisé que des ingrédients analytiques.

Rayon spectral vs norme subordonnée On présente ici les relations à connaître (autant à l'agrégation interne qu'externe) entre le rayon spectral et la norme subordonnée. On va voir que ces relation peuvent être proches, et même très proches...

7 Matrices et topologie

Critère topologique de diagonalisabilité Sur $\mathbb{C}$, une matrice est diagonalisable si et seulement si sa classe de similitude est fermée pour la topologie d'espace normé de $\mathcal{M}_n(\mathbb{C})$. On montre ce résultat, ainsi que son analogue sur $\mathbb{R}$.

L'intérieur des matrices diagonalisables complexes On montre ici que l'intérieur des matrices diagonalisables complexes est constitué des matrices à valeurs propres simples. Il serait utile de réviser un peu le résultant sur

Continuité du spectre d'une matrice On propose de montrer que les valeurs propres d'une matrice dépendent continûment de celle-ci. Le tout est de donner une bonne formulation (on en donnera deux) de ce résultat.

Un exercice de jury autour de l'exponentielle des matrices complexe On connaît tous à l'agrégation (externe) le développement de l'exponentielle complexe qui se trouve être surjective de $\mathcal{M}_n(\mathbb{C})$ vers $\mathrm{GL}_n(\mathbb{C})$ (mais c'est faux sur $\mathbb{R}$). Une question de jury est la suivante, on sait que le sous-espace des traces nulles s'envoie sur $SL_n(\mathbb{C})$ par l'exponentielle. Est ce que l'application ainsi définie reste surjective ?

L'image de l'exponentielle réelle. On fait le point (barre) ! On présente tout les outils pour comprendre si une matrice réelle donnée est ou non l'exponentielle d'une matrice réelle. Tous les outils sont bons pour cette tâche difficile : réduction, polynômes annulateurs, décomposition de Dunford additive, multiplicative. On termine avec un lien peut-être inattendu sur l'étude des structures complexes.

8 - Matrices borderline (à l'agrégation)

Prépa Externe : Matrices échelonnées 1 On commence un nouveau volet sur les matrices échelonnées, qui sont objets mathématiques les plus évitées par les candidats de l'agrégation. Derrière la combinatoire un peu besogneuse du pivot de Gauss se cache le point de départ d'une belle randonnée sur la géométrie de la Grassmannienne. On va essayer de vous faire aimer cette théorie en ne dévoilant que, d'une part, la partie technique mais rassurante de la méthode du pivot et d'autre part la partie à la fois simple et profonde de la géométrie de l'ensemble des sous-espaces de dimension fixée de K^n.

Prépa externe : Matrices échelonnées 2 On a énoncé une bijection entre l'ensemble des matrices échelonnées réduites en colonnes de taille (n, m) et la grassmannienne de sous-espaces de dimension m de $\mathbb{K}^n$. On va montrer ici la surjectivité. On pourrait juste dire qu'il s'agit juste du fameux pivot de Gauss en colonnes. Mais pour être plus précis, on met en place ce pivot : tout d'abord, on en décrit une version en termes de multiplication à droite par des matrices de transvection-dilatation-permutation de GL_m, ce qui nous permet de montrer de façon effective la surjectivité.

Prépa externe : Matrices échelonnées 3 On attaque maintenant l'injectivité, et pour cela on veut retrouver de façon intrinsèque une matrice échelonnée à partir d'un sous-espace de $\mathbb{K}^n$ de dimension m. Dans cette vidéo, on expose la stratégie de la preuve de l'injectivité, puis on montre le premier point : retrouver le « type » de la matrice échelonnée juste à partir du sous-espace.

Prépa externe : Matrices échelonnées 4 On finit la preuve du théorème principal sur les matrices échelonnées, c'est à dire la bijection entre grassmannienne et ensemble de matrices échelonnées. On donne ensuite un exemple sur un corps fini, où on exhibe deux façons de dénombrer une grassmannienne. Une première avec une fraction rationnelle et une autre avec un polynôme.

Méthode QR- exemples, preuves, et petits calculs sur SAGE Voici un algorithme qu'il est bon de connaître pour plusieurs raisons : 1) il est d'une efficacité redoutable pour trouver une approximation de racines de polynômes, 2) la preuve est élégante et 3) dans le contexte actuel, il peut faire l'objet d'un développement dans le contexte d'une leçon à l'agrégation externe (incontournable dans la leçon 149).

Référence : *P*. Ciarlet, Introduction à l'analyse numériue matricielle et à l'optimisation

La dualité dans le théorème de Frobenius Un beau développement dans une leçon sur la dualité consiste à prouver que, dans le contexte des endomorphismes, si le sous-espace u-stable engendré par un vecteur x de E est de dimension le degré du polynôme minimal de u, alors ce sous-espace possède un supplémentaire u-stable. On donne une preuve où l'on motive la nécessité de la dualité.

La désingularisation de Springer du cône nilpotent L'ensemble des matrices nilpotentes de $\mathcal{M}_n(\mathbb{C})$ est un cône possédant des singularités. Et c'est bien ça qui est embêtant ! Springer propose une façon assez naturelle de désingulariser ce cône en associant à chaque matrice nilpotente l'ensemble des drapeaux complets qu'elle respecte.

Nombre d'orbites de matrices entières d'ordre fini A la suite d'une discussion avec Adem Zeghib, voici une façon d'approcher le nombre de classes de similitudes de matrices d'ordre fini dans $\mathrm{GL}_n(Z)$.

Trigonalisation- l'exercice coup de coeur C'est un exercice (en plusieurs étapes) qui s'adresse aux candidats à l'agrégation externe. On montre que si G est un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_p)$, et que tout g de G a un spectre réduit à 1, alors les éléments de G sont simultanément trigonalisables. Au programme : trigonalisation, lemme de Cauchy, dénombrement de $\mathrm{GL}_n(\mathbb{F}_p)$, et enfin, théorèmes de Sylow !

Un théorème bien frais sur le rang et la réduction

Plein d'astuce, plein de ressources dans sa preuve, un théorème qui relie la stabilité de GL_n et celle du rang pour un endomorphisme de $\mathcal{M}_n(\mathbb{C})$.

Isomorphismes qui conservent les matrices de rang 1

La preuve instructive à plus d'un titre d'un petit théorème sur les morphismes de l'espace des matrices qui conservent l'ensemble des matrices de rang 1. Tout d'abord une stratégie générale sur les endomorphismes qui conservent une partie non linéaire, en cherchant les sous-espaces maximaux inclus dans cette partie. Ensuite, l'exercice fait visiter tout ce que l'on a à bien connaître sur les matrices de rang 1. On termine sur un petit épilogue sur les SETIM.

1.4.3 Déterminant droit devant

Un calcul de déterminant (sans les mains)

On se propose de calculer le déterminant de la représentation réelle d'une matrice complexe. Selon comment on attaque ce déterminant, le calcul peut devenir inextricable... ou simple comme bonjour.

Exercice sur la leçon « déterminant »

Sur la leçon déterminant, un type d'exercice dans la discussion avec le jury consiste à vérifier si le candidat a bien compris l'importance et l'utilisation de l'unicité, à scalaire près, d'une n-forme linéaire alternée sur un espace vectoriel de dimension n. L'exercice que l'on présente ici fait est emblématique de ce type de question.

Volume de la n-boule et intégrale de Wallis

Comment évolue le volume de la boule de rayon 1 en dimension n ? Pour $n = 1$, on a $V = 2$, pour $n = 2$, le merveilleux nombre pi, et pour $n = 3$, le célèbre $4/3pi$. Et quelle est sa limite quand n tend vers l'infini ?

Irréductibilité du déterminant (good proof/bad proof)

On va montrer de deux manières que le déterminant vu comme polynôme à n^2 indéterminées, est irréductible. Une première preuve, élémentaire, mais trop simple pour être honnête. Puis, une seconde preuve qui nous amènera sur les sentiers arpentés de la géométrie algébrique et le théorème des zéros de Hilbert.

Déterminants dans le triangle de Pascal (et lemme de Gessel-Viennot)

On va calculer à l'aide de la combinatoire des chemins, le déterminant d'une matrice inscrite dans le triangle de Pascal ! On va prouver pour cela le petit lemme (de grande destinée) de Gessel-Viennot.

Déterminant et polynômes de Lagrange

On construit une matrice carrée à partir de polynômes de Lagrange (non normalisés) et on voudrait en calculer le déterminant. On va voir trois méthodes élégantes se décliner autour de cette taupinade.

Formule de Binet-Cauchy (par la face sud)

La formule de Binet-Cauchy (que l'on peut trouver dans Histoires Hédonistes de Groupes et de Géométries, tome 2, Chap. II) peut être placée avec brio dans une leçon sur le déterminant. On propose une méthode douce pour cette formule dont nous verrons plus tard des applications.

Le théorème du confinement

On prouve qu'il n'y a rien de mieux que le n-gone régulier pour nous protéger de la contagion. Au programme, inégalité d'Hadamard pour les déterminants, et identités de Newton.

Déterminant et combinatoire (formule de Cayley)

On présente ici un joli théorème qui nous permet, à l'aide d'un déterminant, de calculer le nombre de façons de connecter n points de façon minimale. C'est une formule due à Arthur Cayley.

Moore, un nouveau Vandermonde ?

Le déterminant de Moore est non seulement un exercice ludique et passionnant qui demande juste un minimum de connaissance sur les corps finis, mais c est surtout un résultat qui en a sous le capot puisque qu il se situe à l'orée de la profonde théorie de Dickson sur les invariants modulaires. On donnera un aperçu de cette théorie sur laquelle on reviendra reviendra dans une autre vidéo.

Théorème de Descartes- une preuve de 2022 !

Alden Bradford a récemment trouvé une preuve express du théorème de Descartes sur les cercles tangents. Cette preuve utilise une astucieuse interprétation du déterminant de Cayley-Menger.

Log-concavité du déterminant

La log-concavité du déterminant est au coeur d'une belle histoire qui se prolonge jusqu'à la mesure de Hajar sur un groupe de Lie compact, mais nous n'irons pas plus loin dans cet effet d'annonce. Nous nous contentons de prouver cette propriété dans le cadre de l'agrégation interne et externe de mathématiques...

1.4.4 Corps finis à l'envi

Les classes de similitude en dimension 2 (sur corps fini)

Rien de mieux pour comprendre les classes de similitude que de les décrire en totalité dans l'espace des matrices $\mathcal{M}_2(\mathbb{K})$ et de les dénombrer dans le cas où le corps est fini. Une vidéo qui se vit comme un beau voyage, sans (trop d') émission de CO2, et dont on se sort grandi.

Nombre de matrices diagonalisables sur un corps fini (et comportement asymptotique)

Un petit développement pour l'externe. En suivant Carnet de Voyage en Algébrie, on calcule de nombre de matrices diagonalisables sur un corps à q éléments. On en déduit que la probabilité de piocher une matrice diagonalisable dans $\mathcal{M}_n(K)$ tend vers $1/n!$ dans $\mathbb{K}$ est grand.

Sous-espace de matrice diagonalisables sur $\mathbb{F}_p$

On cherche un contre - exemple de sous-espace de matrices toutes diagonalisables sur un corps fini, sans la condition de codiagonalisabilité.

Nombre de matrices nilpotentes sur un corps fini

Le cardinal du cône nilpotent sur un corps fini fournit une formule bien intrigante (c'est le cardinal d'un espace vectoriel du corps fini alors que tout le monde sait que ce cône n'est pas un sous-espace vectoriel !). On tente une méthode sous forme « développement 15 minutes » que l'on peut trouver dans H2G2 tome 2(2015) Chapitre IV-Théorème 4. 1. Une autre méthode est disponible dans Carnet de Voyage en Algébrie, en utilisant le lemme de Fitting.

Nombre de matrices semi-simples sur un corps fini. Comportement asymptotique.

On va attaquer un problème un peu ardu, mais qui ne demande que des choses solubles dans l'agrégation. On va montrer que la probabilité de choisir une matrice semi-simple dans $\mathcal{M}_n(K)$ avec $\mathbb{K}$ fini, tend vers 1 quand le cardinal de $\mathbb{K}$ tend vers l'infini. Le plus long finalement dans la preuve est de faire un inventaire des pré-requis.

Errata : petite coquille à $13'30''$. Il faut mettre un factoriel à a_j (lambda) au dénominateur.

Dénombrement et réduction sur un corps fini-quelques séries génératrices

On résume ici les formules de dénombrement trouvées dans les vidéos précédentes (matrices diagonalisables, nilpotentes, semi-simples) sur un corps fini. On ajoute, pour le plaisir, les matrices trigonalisables, et des versions synthétiques sous forme de séries génératrices.

Corps finis. Construction par les corps de rupture.

On construit généralement le corps fini $\mathbb{F}_q$ comme corps de décomposition du polynôme $X^q - X$. Voici une construction qui ne part de rien (ou presque) et construit le corps $\mathbb{F}_q$ comme corps de rupture d'un polynôme irréductible de degré n sur $\mathbb{F}_p$, avec $q = p^n$.

Questions autour de l'automorphisme de Frobenius

L'automorphisme de Frobenius possède bien des aspects : c'est un morphisme de corps, mais aussi un endomorphisme d'espace, un morphisme de groupes multiplicatif, voire une simple permutation d'ensemble fini. *A* tous ces aspects correspondent des questions classiques, quel est son polynôme caractéristique, est-il diagonalisable, quelle est sa signature, sa décomposition en cycles... Ces questions peuvent désarçonner le candidat à l'agrégation. On tentera de mettre en place quelques réflexes vitaux, et autres gestes-barrière.

1.5 Les groupes sous tous les angles (35)

1.5.1 1 - Groupes finis

Critère de cyclicité pour les groupes finis

Les groupes cycliques sont les « sous-groupes élémentaires » d'un groupe fini. il est donc important de bien les connaître et savoir les reconnaître. On donne ici un critère pour montrer qu'un groupe est cyclique ayant des applications intéressantes, en particulier dans l'étude du groupe multiplicatif d'un corps ou des inversibles d'un anneau intègre. La preuve utilise une formule sur la fonction indicatrice d'Euler, qui elle-même utilise l'étude des groupes cycliques. On tourne en boucle !

Les classes de conjugaison du groupe S_n

Voici une preuve à bien connaître dans la leçon sur les groupes de permutation : celle du théorème qui stipule que deux permutations sont conjuguées si et seulement si elles ont même partition associée. On va partir de la formule de conjugaison des permutations pour définir cette partition associée, et montrer qu'il s'agit bien de ce que l'on appelle un « invariant total de conjugaison ». Invariant total, vous ne viendrez plus chez nous par hasard !

Les classes de conjugaison du groupe S_n-2

Nous venons de voir dans une vidéo précédente que les classes de conjugaison de S_n étaient paramétrées par les partitions de n. Voici maintenant une preuve pour la formule du cardinal de la classe de conjugaison associée à une partition.

Sous-groupe d'indice premier minimal

On montre ici que, **si p est le nombre premier minimal divisant l'ordre d'un groupe G et si H est un sous-groupe d'indice p de G, alors H est distingué dans G**. Ce sera l'occasion de montrer **l'utilité de l'action de G sur l'espace, dit homogène, G/H**.

Groupes de permutations : la surjection de S_n sur S_{n-1}

Le thème des morphismes surjectifs de groupes entre le groupe de permutation S_n et le groupe S_{n-1} permet de visiter tout un pan de la théorie des groupes. A ce titre il tient une place de choix dans les questions de jury et autres divertissements : -)

Moyenne et variance du nombre d'invariants par la formule de Burnside

On sait que le groupe de permutation S_n agit sur l'ensemble des entiers de 1 à n. Combien une permutation $a - t - elle$, en moyenne, d'éléments fixés ? Et quelle en est la variance ? Nous allons voir que toutes les réponses à ces questions proviennent de la formule de Burnside...

Le collier de perles ou le coloriage du n-gone

Voici une présentation du collier de perles en deux parties. Il s'agit dans un premier temps de problèmes de dénombrement modulo action d'un groupe cyclique.

Dans un deuxième temps, on répond à une question très naturelle des coloriages du n-gone modulo isométrie et non plus modulo rotation. Ceci nous mène à observer le groupe diédral, on finit sur une formule générale du nombre de coloriage, qui distingue le cas pair et le cas impair.

La formule de Dobinski (finie)

Une formule qui illustre parfaitement la puissance des actions de groupes. On part de la question suivante : on sait que le groupe de permutation S_n agit transitivement sur $X = [1, n]$. Combien y a-t-il d'orbites quand il agit naturellement sur X^m ?

Oral-ENS sur les permutations

Une petite formule sur les permutations proposée aux oraux l'Ulm. Et une résolution particulièrement sympathique qui passe par toutes les validations d'un programme d'algèbre linéaire de licence : -)

Errata : il faut changer le $-3/4$ en $3/4$ et le $(-1)^n$ en $(-1)^{n+1}$. Merci à Pascal Mathieu de l avoir signalé.

Exercice Oraux-X ENS sur les groupes par Luca

Luca revient nous voir sur la chaîne avec un exercice inédit sur les groupes qu'il a concocté à partir d'un souvenir de $L3$. Les automorphismes de groupes agissent bien sûr naturellement sur le groupe, mais que peut-on espérer de la transitivité de cette action (quand on enlève l'élément neutre) ?

Log discret et protocole El Gamal

On présente le protocole El Gamal et l'intérêt de calculer le logarithme discret afin de décrypter les messages. Cela nous donnera l'occasion de voir ou de revoir les techniques de base dans un groupe cyclique...

Les groupes d'ordre 8 par Luca

Luca nous propose une preuve de la classification des groupes d'ordre 8 au niveau licence.

Groupes hamiltoniens et théorème de Dedekind

On présente ici la classification des groupes hamiltoniens finis, c'est-à-dire des groupes finis dont tous les sous-groupes sont distingués. La preuve est juste lumineuse, tout en utilisant des outils élémentaires.

Un groupe dont tous les sous-groupes sont distingués

On sait que les groupes abéliens partagent cette propriété que tous leurs sous-groupes sont distingués. Mais sont-ils les seuls ? Nous proposons ici un modèle de groupes non abéliens finis qui vérifient également cette propriété. Un théorème de Dedekind nous affirme que ce sont les seuls. Mais en attendant le théorème d'unicité, il s'agit d'un exercice bien agréable qui nous fait visiter les propriétés si particulières du groupe des quaternions.

Théorème de Jordan-Schur (sous-groupes finis de GLn(C))

On montre que les sous-groupes finis de $\mathrm{GL}_n(C)$ ne sont "pas bien méchants". Ils possède un sous-groupe distingué abélien d'indice borné par une fonction f(n). C'est le théorème de Jordan et Schur. On décompose la preuve en petits exercices, comme on le ferait pour un problème d'agrégation !

1.5.2 2 - Sous-groupes de GLn- groupe orthogonal

Le groupe orthogonal (engendrement en toute simplicité)

Pas description, tout est dans la vidéo.

Tout (ou presque) sur le groupe orthogonal !

On va faire le point sur le groupe orthogonal : définitions, premières propriétés, centre, sous-groupes distinguées, réduction, topologie, actions... Mais bien entendu, le groupe orthogonal, c'est aussi un groupe qui participe à des décompositions (polaires, QR) essentielles en mathématiques !

Sous-groupes compacts de $\mathrm{GL}_n(\mathbb{R})$

On va montrer, dans un premier temps, que **le groupe orthogonal est compact** et, même, qu'**il s'agit d'un sous-groupe compact maximal de $\mathbf{GL_n(R)}$.** Dans un deuxième temps, on va passer à un théorème plus difficile mais fondamental : **tout sous-groupe compact est conjugué à un sous-groupe de $\mathbf{O_n}$**. Ce morceau de bravoure **nous demandera d'utiliser le théorème de l'ellipsoïde de John-Loewner**. Voir le chapitre des développements.

Sous-groupes à 1 paramètre de $\mathrm{GL}_n(\mathbb{C})$

On présente un développement qui peut être utile également aux épreuves écrites (voir Agreg interne EP1-2014) sur les morphismes continus du groupe additif $\mathbb{R}$ vers $G_n(\mathbb{C})$. On suit l'exercice III-F-17 de Nouvelles Histoires Hédonistes de Géométries.

1.5.3 3 - Groupes en analyse

Sur le groupe des homéomorphismes de $\mathbb{R}$

Quelques aspects « groupistes » de l'ensemble des homéomorphismes de $\mathbb{R}$, muni de la loi o. On s'intéresse ici à un objet essentiellement analytique, mais avec un regard d'algébriste.

1.5.4 4-Groupes en action borderline :

Un théorème de Jordan sur le groupe linéaire modulo n

Un petit théorème de Jordan qui nous emmènera sur les rivages du groupe linéaire $\mathrm{GL}_k(Z/nZ)$ et qui vient généraliser l'indicatrice d'Euler (pour $k = 1$). On pourra voir dans ce théorème une extension du domaine du lemme chinois !

Tout sur le groupe dérivé- $1/2$

On fait le point sur ce qui est bon de connaître sur le groupe dérivé à l'agrégation externe. Dans un premier temps, on va voir les notions de commutateur, de sous-groupe dérivé, et les propriétés basiques de ces sous-groupes. On continue avec tous les exemples à connaître des groupes dérivés des groupes classiques.

Tout sur le groupe dérivé- $2/2$

Dans cette seconde partie, on calcule encore deux sous-groupe dérivé : celui du groupe alterné A_4 et du groupe spécial linéaire $SL_2(\mathbb{F}_3)$. On attaque des application : l'utilisation du groupe dérivé dans les groupes simples d'ordre 60, l'étude des morphismes de $G_n(K)$ dans le groupe K^*, la non existence d'un sous-groupe d'indice 2 dans A_4 et un contre - exemple qui prouve que $D(G/H)$ n'est en général pas isomorphe à $D(G)/D(H)$.

Les groupes ? Optez pour la simplicité.

Pour les oraux d'agrégation externe, si l'on a montré lors d'un développement que tel ($SO3$) ou tel (A_n) groupe est simple, il n'est pas mauvais de pouvoir expliquer pourquoi cet engouement pour les groupes simples. Cette vidéo est là pour nous donner bon nombre d'application à la simplicité.

Y a-t-il un sous-groupe d'indice 2 (dans l'avion) ?

On part d'une question d'apparence anodine : parmi les groupes classiques, quels sont ceux qui possèdent des sous-groupes d'indice 2. Cette question nous amène à tout un florilège de groupes classiques et surtout à un arsenal de moyens qu'il est bon de dominer à l'agrégation. Pour n'en citer que quelques uns : réciproque de Lagrange dans le cas cyclique, théorème de structure des GAF, sous-groupes dérivés, signature, systèmes de générateurs de A_n, de SL_n, formes linéaires, cyclicité du groupe multiplicatif d'un corps fini, transvections, morphisme déterminant, sous-groupe dérivé de SO_n, et le feu d'artifice final, la norme spinorielle !

L'exposé ne serait pas complet dans la propriété qui dit qu'un sous-groupe d'ordre $2n$, n impair, possède toujours un sous-groupe d'indice 2. Voir la vidéo `https://youtu.be/gBFdv08p7Nc`

Merci à Nicolas Vichery de me l'avoir fait remarquer.

Sous-groupes finis de $\mathrm{GL}\,2(R)$ et $\mathrm{GL}\,2(Z)$

Voici dans le cadre de l'agrégation externe, un petit théorème sur la classification des sous-groupes finis de $\mathrm{GL}_2(\mathbb{R})$ et $\mathrm{GL}_2(\mathbb{Z})$.

Morphismes entre groupes abéliens finis (la Saga des GAF)

On propose de comprendre les groupes d'automorphismes des groupes abéliens finis. On met en place dans un premier temps quelques résultats élémentaires et classiques : groupe de morphismes entre groupes cycliques, interprétation de la composition, mise en forme matricielle.

On continue avec le second volet où l'on résout les exercices annoncés (de la liste de Damien Mégy pour l'agrégation externe) dans le premier volet. Quels sont les groupes d'automorphismes de $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ et de $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$? On propose une méthode qui permet au final de comprendre le cas général : pouvoir décrire les groupes d'automorphismes d'un groupe abélien fini quelconque !

Utilisation des configurations en théorie des groupes

Sur l'exemple de la configuration de Cremona-Richmond, on propose de donner un exemple édifiant de l'utilisation des configurations pour mieux comprendre certains groupes finis. En réalisant une configuration via deux « géométries » différentes, on peut réaliser de deux manières le groupe des automorphismes de la configuration et relier ainsi deux groupes finis classiques. On présente ensuite des situations analogues avec le plan de Fano et la configuration de Desargues. La présentation est un diaporama de ma collaboratrice Marie Péronnier et le texte provient d'un travail conjoint avec Jérôme Germoni dans le tome 2 d'Histoires hédonistes de groupes et de géométries.

Isomorphismes exceptionnels de groupes finis-1/2

On motive ici le problème des isomorphismes entre les groupes linéaires et groupes de permutations, en suivant le livre Nouvelles Histoires Hédonistes de groupes et de Géométries. Ces problèmes ont animés de grands mathématiciens, de Galois, dans sa lettre testamentaire, $jusqu'aux$ grands mathématiciens du XXième siècles qui ont façonné la classification des groupes simples finis. Désormais, ces problèmes intéressent également nos étudiants à l'agrégation dans leur préparation de développements !

Isomorphismes exceptionnels de groupes finis-2/2

On attaque ici le cas des isomorphismes dits exceptionnels pour les corps $\mathbb{F}_4$, et $\mathbb{F}_5$. On conseille, pour ceux qui seraient intéressés de les comprendre tous (!) la lecture du chapitre XII de Histoires hédonistes de groupes et de géométries (2015)

Construire un automorphisme extérieur de S_6

Les actions de groupes permettent de construire des morphismes d'un groupe G vers un groupe de permutation S_n. Il suffit d'une belle coïncidence numérique pour construire un morphisme de S_n dans lui-même. Pour $n = 6$, on prouve que l'automorphisme obtenu est extérieur (ie. n'est pas intérieur).

Représentations de groupes et géométrie- Présentation 1

Cette vidéo est une présentation des vidéos qui vont suivre. On y explique un schéma généaral fécond entre représentations, classes de conjugaison et géométrie. Le but ici est double : présenter d'une part un développement sur les groupes à table de caractères entière (dont fait partie le groupe de permutations S_n) et l'ubiquité du nombre d'or à travers divers point de vue : algébrique, géométrique, théorie de Galois, et enfin dans les classes de conjugaison des groupes finis, via la théorie des représentations.

Représentations de groupes et géométrie- Table de caractères de S_n-2

On attaque donc un critère permettant de voir si la table de caractère d'un groupe fini est à valeurs dans $\mathbb{Z}$. On passe par un petit lemme sur les extension cyclotomiques, puis, une étude des classes de conjugaison de S_n. Curieusement, les choses s'enchaînent sans nécessiter de connaissances particulières sur la théorie des représentations.

Représentations de groupes et géométrie- le nombre d'or en géométrie et en théorie des corps-3

On commence notre traque au nombre d'or phi. Tout d'abord, dans les équations algébriques, puis dans la géométrie (avec le pentagone régulier et l'icosaèdre) et enfin dans la théorie des corps. Nous prouverons une caractérisation, dont nous aurons besoin par la suite, des éléments de Q (omega) (où omega est une racine primitive 5ème de l'unité) qui s'écrivent sous la forme $a * \phi + b$, avec a , b rationnels et a non nul.

Représentations de groupes et géométrie- le nombre d'or dans D_5 et A_5 -4

On voit comment apparaît le nombre d'or dans les classes de conjugaison de groupes finis via la théorie des représentations. Ici, on le voit sur l'exemple des groupes D_5 et A_5.

Origines de la théorie des représentations 1/2

Un résumé de l'excellent article « tout public » (!) de Keith Conrad « the origin of representation theory » que l'on peut trouver sur sa page web. On y découvre comment la factorisation d'une matrice circulante générique a permis à Dedekind d'aboutir au problème de déterminant d'une table de groupe, résolu il y a 120 ans par Frobenius, donnant ainsi naissance à la théorie des représentations.

Origines de la théorie des représentations 2/2

Un résumé de l'excellent article « tout public » (!) de Keith Conrad « the origin of representation theory » que l'on peut trouver sur sa page web. On y découvre comment la factorisation d'une matrice circulante générique a permis à Dedekind d'aboutir au problème de déterminant d'une table de groupe, résolu il y a 120 ans par Frobenius, donnant ainsi naissance à la théorie des représentations. Dans ce second volet, on s'inspire du calcul pour le groupe symétrique S_3 pour comprendre la situation générale.

Coloriages et théorie des représentations

On a trouvé une formule élégante, due à Polya, qui permettait de calculer assez facilement le nombre de coloriages possibles d'un ensemble X, modulo une action de groupes. Dans cette vidéo, on transforme cette formule en une formule équivalente, traduite en termes de théorie des représentations pour le groupe des permutations de X. On constate avec bonheur que la théorie de coloriages permet une introduction naturelle des polynômes de Schur, Graal des combinatoristes et des théoriciens de représentations. On illustre toute cette jolie théorie sur un exemple courant. $P.\ S.$ cette vidéo ne demande pas une grande familiarité à la théorie des représentations, mais son but non avoué est de participer à cette familiarité !

Formule d'Erdös-Turan pour les classes de conjugaison de A_n

Une prouesse signée Erdös et Turan pour cette preuve élégante de la formule qui calcule le nombre de classes de conjugaisons du groupe alterné A_n à l'aide de la fonction partition.

Heisenberg ou l'incertitude des GAF

Trois fonctions pour une seule vidéo ! Bien sûr, prouver l'inégalité appelée « principe d'incertitude d'Heisenberg » dans le cadre des groupes abéliens finis, et aussi, d'expliquer brièvement en quoi elle est reliée au fameux principe d'incertitude qui sévit en physique quantique. Mais avant tout, on pourra la voir comme un plaidoyer pour la réinsertion des groupes abéliens finis dans les programmes de licence.

Produit semi-direct- une introduction en douceur

Voici une introduction en douceur des produits semi-directs, dans le sens que 1. on ne parle pas de suite exacte, 2. on commence sur des exemples en petits cardinaux, 3. On parle de produits semi-directs internes avec des exemples dans la nature, 4. On généralise au cas externe sans preuve calculatoire...

Isomorphismes de produits semi-directs (le contre-exemple)

Après avoir redéfini le produit semi-direct de deux groupes, on donne une première situation assez générale qui assure l'isomorphisme de PSD. On montre ensuite un contre-exemple qui prouve qu'on n'est loin d'avoir tout compris à partir de cette situation...

1.6 Arithmétique, anneaux, corps et polynômes (50)

1.6.1 Arithmétique (19)

Deux équations diophantiennes quadratiques

On propose deux équations diophantiennes de type $x^2 + y^2 - pz^2 = 0$, où p est un nombre premier. Dans un premier temps p est congur à 3 modulo 4, et l'équation est vite résolue. Dans un deuxième temps, p est congru à 1 modulo 4 et, après avoir fait des rappels sur la factorialité de $\mathbb{Z}[i]$, on en trouve toutes les solutions.

Le problème des diviseurs de Dirichlet

Trouver quel est le nombre de diviseurs (positifs) d'un entier donné est chose facile, mais quelle est la moyenne du nombre de diviseurs sur les n premiers entiers consécutifs est chose plus ardue et pourrait même nous emmener vers des des fonds abyssaux. Voici un petit exposé du problème (en deux volets) qui peut constituer un développement raisonnable à l'agrégation interne (ou externe), vu ses liens avec l'analyse et l'arithmétique..

Le problème des diviseurs de Dirichlet-2

(Seconde et dernière partie) Trouver quel est le nombre de diviseurs (positifs) d'un entier donné est chose facile, mais quelle est la moyenne du nombre de diviseurs sur les n premiers entiers consécutifs est chose plus ardue et pourrait même nous emmener vers des des fonds abyssaux. Voici un petit exposé du problème (ne deux volets) qui peut constituer un développement raisonnable à l'agrégation interne (ou externe), vu ses liens avec l'analyse et l'arithmétique..

Une formule polynomiale pour l'identité de Bezout

Algorithme d'Euclide et polynômes continuants

Nous allons voir ici des formules polynomiales qui permettent, entre autres, de calcul une identité de Bezout entre deux nombres a et b à partir de l'algorithme d'Euclide. On introduit des polynômes classiques, que l'on peut voir comme des analogues polynomiaux des nombres de Fibonacci. Dans un deuxième temps, nous allons utiliser ces polynômes continuants définis pour donner une borne au nombre d'opérations à effectuer à partir de deux nombre a et b dont on veut trouver le pgcd. Une recherche qui nous fera découvrir la base d'or...

Divisibilité dans les nombres de Fibonacci et de Lucas-1

Un petit exposé de Denis Roussillat. Pour un nombre premier p fixé, Denis étudie la condition « p divise F_n » et « p divise L_n », où (F_n) et (L_n) désignent respectivement la suite de Fibonacci et la suite de Lucas, cette dernière étant à la première ce que le sinus est au cosinus. Dans un premier temps, après avoir fait quelques remarques d'ordre empirique, on explique une jolie propriété de périodicité pour la première condition.

Divisibilité dans les nombres de Fibonacci et de Lucas-2

Et voici un critère portant sur le rang pour qu'un nombre premier divise un nombre de Lucas.

Divisibilité dans les nombres de Fibonacci et de Lucas-3

On veut montrer que l'ordre $b(p)$ d'apparition d'un nombre premier p dans la suite de Fibonacci divise $p-1$ ou $p+1$ selon les congruences de p modulo 5. Même si on pourra trouver des méthode plus directes, celle-ci fait visiter un bon nombre de parties du programme de l'agrégation et peut devenir un joli développement. Au programme : nombre premiers, corps finis, et formes quadratiques.

Lemme chinois- le best off

(Compil.) Un recueil d'exercices autour du lemme chinois en arithmétique (et autres mandarinades)

Un exercice qui utilise le lemme chinois

Un petit exercice qui a l'avantage de faire le point sur toutes les techniques autour du lemme chinois. Combien y a-t-il d'entiers premiers à 120 et congrus à 3 modulo 4 ?

Exercices de confinement Arithmétique 1

Voici quelques petits exercices corrigés en arithmétique. Des exercices que l'on peut poser à l'oral, donc généralement plus facile que des exercices d'écrit. Au programme, le théorème fondamental de l'arithmétique, le lemme de Gauss, la fonction d'Euler, le théorème de Lagrange... On ne donne pas d'équations diophantiennes (celles-ci sont déjà dans la playlist « exercices d'arithmétiques »).

Exercices de confinement Arithmétique 2

On résout des petits équations de congruence autour du lemme chinois, puis, lorsque le lemme chinois ne peut pas nous venir en aide (on travaille modulo 17^2), on a une variante avec une méthode de Newton p-adique. Enfin, deux exercices supplémentaires autour de la fonction indicatrice d'Euler.

Exercices de confinement Arithmétique 3

On revient sur les systèmes (affines) de congruences. On attaque les systèmes à trois équations et le cas où l'on sort du cadre classique du lemme chinois, c'est-à-dire, où les nombres ne sont pas premiers entre eux.

Exercices de confinement Arithmétique 4

On résout un petit système de congruence dans un cadre « hors lemme chinois » avant de modéliser ce type de système sous forme de suite exacte de groupes.

Loi complémentaire de réciprocité quadratique au bac !

La loi complémentaire de réciprocité quadratique a été donnée au bac marocain 2023 sous forme d'exercice. Voici donc ce qui est probablement la preuve la plus élémentaire du fait que le résidu quadratique de 2 modulo p premier impair est égal à $(-1)^{(p^2-1)/8}$.

Codage RSA, décodage et cryptanalyse

Comme application classique du lemme chinois, on présente ici le codage RSA, son décodage, avec un exemple. Moins classique, nous allons présenter dans cette vidéo des tentatives de craquage du code, Tout d'abord, ce que l'on appelle l'attaque de Fermat. Puis, on étudie l'efficacité d'une attaque probabiliste du système RSA.

Au programme : le lemme chinois, qui nous permet de résoudre une équation algébrique dans $\mathbb{Z}/n\mathbb{Z}$.

Système RSA-1 Codage et décodage

On présente le système RSA : codage, décodage et cryptanalyse (comment casser le code ?) en trois vidéos, le tout dans le cadre d'un oral à l'agrégation. Cette première vidéo traite du codage et du décodage.

Errata : J'ai écrit par mégarde une coquille : phi $(n) = (p-1)(q-1) = n-p-q-1$ au lieu de $n-p-q+1$. Je dois un coup à boire à Sébastien Sanchez qui me l'a signalée

Système RSA-2 Attaque de Fermat et attaque probabiliste

On présente le système RSA : codage, décodage et cryptanalyse (comment casser le code ?) en trois vidéos, le tout dans le cadre d'un oral à l'agrégation. Cette seconde vidéo traite de l'attaque, dite, de Fermat, et d'une autre forme d'attaque, plus empirique.

Errata : J'ai écrit par mégarde une coquille : phi $(n) = (p-1)(q-1) = n-p-q-1$ au lieu de $n-p-q+1$. Je dois un coup à boire à Sébastien Sanchez qui me l'a signalée

Système RSA-3 Attaque de Wiener

On présente le système RSA : codage, décodage et cryptanalyse (comment casser le code ?) en trois vidéos, le tout dans le cadre d'un oral à l'agrégation. Cette troisième vidéo traite de l'attaque de Wiener, basée sur le théorème de meilleure approximation, que nous nous contenterons d'énoncer ici, mais que nous démontrerons dans une prochaine vidéo.

Errata : en fait, tout à la fin je dis que l'on doit vérifier que x^d est congru à x modulo n, mais c'est $(x^e)^d$ qui doit être congru à x modulo n

La fonction totient de Jordan

On introduit cette fonction de l'arithmétique, due à Jordan, qui généralise l'indicatrice d'Euler en « dimension $\mathbb{K}$ ». On utilisera, comme c'est souvent le cas avec les fonctions arithmétiques, la convolution de Dirichlet ainsi que la fonction de Moebius.

La constante d'Hermite

Un développement que l'on pourra retrouver avec bonheur dans « 131 développements pour l'oral ». Le point de départ est, à partir d'une forme quadratique définie positive q, trouver le minimum de $q(x)$ pour x entier non nul. Mais ce problème s'avère difficile et il est plus raisonnable d'approximer ce min à l'aide du déterminant de la forme q. Un joli développement donc, avec des petites techniques instructives pour l'agrégation (pivot dans un cadre symétrique, existence d'un min sur un discret... pour la ref !

Le théorème de Wilson en 4 preuves et une application !

On propose ici pour le théorème de Wilson, quatre preuves assez différentes pour pouvoir nous donner un aperçu des méthodes en arithmétique allant de la terminale (option math) jusqu'à l'agrégation ! On finit avec une petite application classique.

1.6.2 Anneaux (4)

Entiers de Gauss, factorialité, et cercle rationnel.

On introduit tout d'abord la paramétrisation rationnelle du cercle, qui possède l'avantage de pouvoir se définir sur tout corps, contrairement à la paramétrisation trigonométrique, spécifiquement réelle. En comparant les deux paramétrisations sur le corps Q des rationnels, on arrive à se demander quels sont les points rationnels du cercle, dont l'angle associé est commensurable avec pi. On montre que ce sont juste les points cardinaux du cercle. Il se trouve que la factorialité de l'anneau des entiers de Gauss (et ses inversibles) se cache derrière ce phénomène.

Entiers de Gauss, factorialité, et cercle rationnel-2

A l'aide d'une jolie preuve qui utilise l'anneau des entiers de Gauss et sa factorialité, on a montré récemment que les points rationnels du cercle dont l'angle associé est commensurable avec pi sont les quatre points cardinaux. On montre ce même résultat par une autre méthode, proposée par Jérôme Germoni, qui utilise les polynômes cyclotomiques et l'indicatrice d'Euler.

Entiers de Gauss (petits calculs entre amis)

Quelques petits calculs à la bonne franquette dans l'anneau $\mathbb{Z}[i]$ des entiers de Gauss. Un apéro convivial avec au menu division euclidienne, algorithme d'Euclide, identité de Bezout, décomposition en facteurs premiers. On verra de nos propres yeux des idéaux de $\mathbb{Z}[i]$, de nouveaux corps quotients exotiques qui vont nous changer de $\mathbb{Z}/p\mathbb{Z}$. On y va sans complexe, et on se laisse guider par le plaisir !

$X^p - a$ et l'alternative irréductible/existence de racine

Voici la preuve classique du fait que si p est premier $P = X^p - a$ est irréductible sur un corps $\mathbb{K}$ si et seulement si P n'a pas de racine dans $\mathbb{K}$.

1.6.3 Corps (2)

Introduction au corps des quaternions- (X-ENS-2023) -1

Dans cette vidéo, nous allons introduire le corps des quaternions selon le principe que si vous avez compris le corps des complexes, alors, vous avez compris les quaternions... à condition que vous puissiez changer les « o » en « u ».

Epreuve ENS-2023- Introduction au corps gauche des quaternions-2

On continue cette présentation du corps des quaternions en suivant la trame de l'épreuve ENS-2023 (mais en proposant parfois les raccourcis de Nouvelles Histoires Hédonistes-Chap. VII). On y découvre que toute rotation de l'espace de dimension 3 peut être réalisée comme une conjugaison sur l'espace des imaginaires quaternioniques !

1.6.4 Polynômes (10)

Un exercice sur le thème « polynôme, racines et multiplicités »

Un exercice d'apparence anodine sur une racine d'un polynôme P dans $Q[X]$, et une condition nécessaire sur sa multiplicité pour que cette racine soit dans le corps de base (Q). Cet exercice résiste (car il existe !) aux approches naïves, et ce pour une bonne raison : une notion important se cache derrière le corps de base.

Errata (merci à Samir Boufnichel pour son commentaire) il faut dire que le degré de $P'1$ est strictement plus petit que le degré de $P1$ pour affirmer que le polynôme minimal de alpha divise strictement $P1$. En effet, il n est pas clair du tout que $P'1$ divise $P1$ comme je l ai affirmé.

Exercices sur le thème relations coefficients-racines

On propose sept petits exercices divers et variés pour combler les lacunes sur cette thématique fondamentale en mathématiques.

Un petit test sur les racines multiples

On propose un petit exercice sur un polynôme à coefficients entiers dont on impose qu'il possède une racine double. La question est « dans quels corps ceci est-il possible ? ».

Dans un deuxième temps cette question nous amènera à un critère étonnant de primalité et on conclut avec ce qui pourrait être une amorce de problème d'agrégation.

Quand P'' divise-t-il P ?

Voici un petit exercice qui pourrait sembler anodin s'il n'était pas en triple connexion avec un célèbre mathématicien du nom de Gauss ! On cherche les polynômes de $C[X]$ tels que P'' divise P. On vas proposer deux solutions, une élémentaire par les séries entières, une autre par l'algèbre linéaire par la réduction. Mais surtout, Totototo a remarqué un lien avec les fonctions hypergéométriques de Gauss, et finalement cette petite taupinade va se retrouvée cernée de près par le théorème de Gauss-Lucas, les fonctions hypergéométriques et pour finir, les théorèmes de quadrature de Gauss. Bref, le festival de Göttingen !

Un exercice qui utilise des polynômes

Comment, à l'aide de polynômes, prouver que les fonctions x^{a_i} sont indépendantes ? A vous de jouer !

Un exercice sur polynômes et PGCD (Agreg Externe 2021 Spécial docteur)

Un exercice instructif donné à l'AE spécial docteur 2021. Il s'agit de montrer que la suite PGCD $(P(n), Q(n))$ est périodique quand P et Q sont des polynômes à coefficients entiers sans diviseurs communs. En quelques minutes, on parcourt les principales techniques arithmétiques liées au PGCD, et on déjoue quelques gros pièges !

Polynômes interpolateurs de Lagrange vs lemme chinois ?

On présente ici le théorème des polynômes interpolateurs de Lagrange dans une version « lemme-chinois-compatible ».

Décomposition des polynômes cyclotomiques modulo p

On donne ici une description de la décomposition en irréductibles du n-ième polynôme cyclotomique modulo p, un nombre premier. Dans un premier temps, on étudie le cas où p ne divise pas n, puis on s'intéresse au cas général.

Irréductibilité des polynômes cyclotomiques (ma preuve coup de coeur)

La preuve de Issaï Schur de l'irréductibilité des polynômes cyclotomique est pour moi la preuve la plus élégante et la plus instructive, suivie de près de celle que l'on peut trouver dans le livre de Daniel Perrin qui consiste à réduire modulo p une réduction sur $\mathbb{Z}$. On utilise ici les discriminant du polynôme $X^n - 1$ ainsi que l'anneau des entiers algébriques.

Polynômes cyclotomiques (petits calculs entre amis)

On introduit les polynômes cyclotomiques et les deux formules qui permettent de les définir. Une formule qui les définit, mais qui n'est pas pratique d'utilisation, et une formule qui permet de les calculer par récurrence. C'est cette seconde formule qui va nous permettre de faire des petits calculs préliminaires. Le but est de calculer (au moins se rassurer qu'on est capable de le faire facilement) ϕ_n pour n de 1 à 104. Dans cette première vidéo, on se contentera de les calculer jusqu'à 12.

Les petits calculs sur les polynômes cyclotomiques vont ensuite devenir un peu plus sérieux à l'aide de la fonction de Moebius qui va nous formule d'inversion très utile pour passer de ϕ_n à ϕ_{pn} pour tout p premier.

On termine enfin ce petit exposé sur le calcul des polynômes cyclotomiques avec le calcul des polynômes ϕ_{pq}, premiers. On verra une recette simple qui nous permet de trouver tous les monômes de la décomposition, ce qui nous permet de voir, au passage, que si n ne possède que deux facteurs premiers impairs dans sa décomposition (même avec multiplicité) alors, ϕ_n possède tous ses coefficients dans $\{0, 1, -1\}$. Le premier polynôme cyclotomique qui échappe à nos recettes simples sera donc pour $n = 3 \times 5 \times 7 = 105$. On finit sur un exemple en calculant ϕ_{60}.

Calcul d'une série exponentielle

On cherche à calculer explicitement la série génératrice exponentielle d'un polynôme réel. Un exercice qui demande un peu de calcul et également un peu de savoir-faire. En particulier, le choix d'une base adaptée de l'espace des polynômes et la résolution d'un système linéaire.

Friandises avec déterminants et polynômes

Deux petits exercices bien instructifs sur le thème déterminants et polynômes. Au programme, le théorème fondamental des déterminants, Vandermonde, Taylor polynomial, et du doigté ! Au final, pour les experts, on montre comment passer d'une formule algébrique sur un corps de caractéristique nulle vers un corps de caractéristique non nulle...

Le lemme de Hensel pour la factorisation

On présente le lemme de Hensel dans sa version « factorisation de polynômes » mais dans le cadre de l'agrégation et sans parler (sauf pour la culture) des entiers p-adiques. Il n'est pas courant de voir ce lemme en développement à l'agrégation, mais si on le regarde bien, il possède un joli taux de placement !

Le critère d'irréductibilité de Cohn

Voici un critère d'irréductibilité sur $\mathbb{Z}[X]$ qui fera concurrence à celui d'Eisenstein tout en développant un bon nombre de techniques utile dans le monde de l'arithmétique des polynômes. Un théorème étonnant qui finalement ne demande que très peu de bagage.

Kronecker : la méthode à Toto !

Toto, qui intervient de façon pertinente sur cette chaîne propose une variante pour le développement du théorème de Kronecker. Ici, il n'est plus question de relations coefficients-racines mais de l'utilisation du contenu de Gauss dans un lemme classique (mais toutefois instructif).

Factorisation sur Fq et factoriel de Carlitz

Un joli développement (néanmoins classique) consiste à factoriser le polynôme "total" $X^{q^n} - X$ sur $\mathbb{F}_q$. Nous donnons la preuve classique de ce développement mais avec deux applications, dont une plutôt nouvelle à effet waouh : le calcul du factoriel de Carlitz ! Pour une fois qu'un développement, c'est une factorisation, faut en profiter :-))

Qui es-tu, critère d'Eisenstein ?

On décline dans cette petite vidéo les preuves du critère d'irréductibilité d'Eisenstein. Tout d'abord la preuve classique (finalement assez élémentaire), puis, une preuve par passage au quotient. Mais la troisième preuve, bien plus subtile qui utilise de l'analyse p-adique nous montre le critère sous un nouveau jour, permettant de nouvelles extensions...

Irréductibilité sur $\mathbb{Z}[X]$. Un exercice bien pourri (mais instructif !)

Laurent, que je remercie au passage, me fait justement remarquer que l'exercice, lourd d'hypothèses, que j'ai mis récemment en ligne https ://youtu.be/AahMFR4y5Sc, était trivialisable en allégeant complètement les hypothèses. Je fais donc ici un rectificatif, mais en assumant tout de même la méthode, qui contrairement à l'exemple choisi, me semble digne d'être présentée. Elle consiste à utiliser le treillis complet des partitions d'un nombre pour prouver l'irréductibilité d'un polynôme sur un anneau. Le rectificatif nous semble d'autant plus important à faire que cet exercice se retrouve dans deux références importantes de nos agrégatifs.

1.6.5 Arithmétique borderline pour l'agrégation

Exercices de confinement Réseaux 3

On a souvent besoin en arithmétique d'utiliser de choses élémentaires sur les réseaux. A l'écrit, la caractérisation des $\mathbb{Z}$-bases de $\mathbb{Z}^n$ et un « théorème de la $\mathbb{Z}$-base incomplète » peut être souvent utile. C'est ce que l'on va voir dans un petit exercice qui nous fera faire un premier pas dans le monde des réseaux.

1.6.6 Carrés en tout genre (9)

Le théorème des deux carrés par l'approximation rationnelle

Voici une preuve élémentaire du théorème des deux carrés qui utilise un théorème d'approximation rationnelle que l'on a prouvé (également de façon élémentaire) sur cette chaîne, voir `https://youtu.be/bvK7aSUDmjQ`

Les suites de Farey 1/2

Mathématiques récréatives aujourd'hui ! Avec les suites de Farey. Des suites si simples à définir, mais si profondes en conjectures.

Les suites de Farey 2/2

Les suites de Farey. Des suites si simples à définir, mais en ligne rouge avec les approximations de réels par des rationnels, et surtout, avec l'hypothèse de Riemann !

Le théorème des quatre carrés. Décomposition d'un nombre en carrés-1

Un développement technique mais toutefois élémentaire : tout entier naturel peut se décomposer en somme de quatre carrés. On utilisera une méthode de descente de Fermat. On discutera ensuite d'une preuve alternative plus savante qui généralise une preuve du théorème des deux carrés bien connue des agrégatifs !

Le théorème des deux carrés par les réseaux du plan. Décomposition d'un nombre en carrés-2

Une suggestion de notre follower « *Pastix*51 » dont un de ses développements préférés a été cette jolie méthode de géométrie arithmétique pour prouver le théorème des deux carrés.

Décomposition en carrés et réseaux cubiques. Décomposition d'un nombre en carrés-3

A la suite d'une conversation avec *Pastix*51, je constate que les théorèmes de décompositions en carrés peuvent être prouvés élégamment, de façon uniforme, et surtout de façon assez élémentaire, à l'aide de réseaux « cubiques ». En épilogue, dans une tentative d'appel à l'aide, je constate un lien avec les sous-espaces totalement isotropes maximaux (SETIM).

Errata : Mon collègue Pierre Baumann me signale une erreur (rectifiable) dans la preuve du théorème des quatre carrés par les réseaux. Un hypercube en dimension 4 possède un point (unique) intérieur tel que sa distance à un sommet de l'hypercube est égale au côté de l'hypercube. C'est le point central de l'hypercube, qui pourrait être dans le réseau et dans ce cas, l'hypercube ne serait pas un domaine fondamental du réseau. Mais par l'absurde, on voit que si ce point milieu était dans le réseau, le domaine fondamental serait de volume $1/2(x_1^2+x_2^2+x_3^2+x_4^2)^2$ et on aurait $2p^2=(x_1^2+x_2^2+x_3^2+x_4^2)^2$, ce qui est absurde car 2 n'est pas un carré...

Fonctions qui préservent les sommes de carrés par Jamil-1

Trouver les fonctions sur N, qui préservent les sommes de carrés. Un joli petit exercice niveau lycée, ou plutôt olympiades, proposé par mon ancien (et sympathique) étudiant Jamil Berhila, qui continue malgré les années à me vouvoyer et m'appeler monsieur, comme quoi les études, ça laisse des traces ! On résout ici le problème, modulo un lemme qui sera prouvé dans la vidéo suivante.

Fonctions qui préservent les sommes de carrés par Jamil-2

On finit ce joli exercice avec la preuve du lemme. Pythagoriciens, pythagoriciennes, bonsoir !

Loi complémentaire de réciprocité quadratique (un exercice du cours de *D*. Perrin)

Une preuve très simple pour montrer que 2 est un carré modulo p (impair) si et seulement si p est congru à 1 ou -1 modulo 8.

1.7 Les formes quadratiques en éveil (19)

1.7.1 Qui es-tu, forme polaire ?

Une vidéo où l'on présente la forme polaire, en lui posant les trois questions : qui es-tu ? que fais-tu ? d'où viens-tu ? Une vidéo qui aidera a digérer un cours sur les formes quadratiques.

1.7.2 Les « Corona Sessions » de la prépa. Formes de Hankel 1/7

On propose ici une série de vidéos qui expliquent progressivement les formes de Hankel. L'idée est de partir d'un polynôme réel et, juste à l'aide d'identités de Newton et de méthode de Gauss (sur les formes quadratiques), trouver son nombre de racines distinctes et de racines réelles. Une première vidéo pour l'étude d'un cas élémentaire : les racines sont toutes réelles et distinctes, et la forme de Hankel est définie positive.

1.7.3 Les « Corona Sessions » de la prépa. Formes de Hankel 2/7

On propose ici une série de vidéos qui expliquent progressivement les formes de Hankel. L'idée est de partir d'un polynôme réel et, juste à l'aide d'identités de Newton et de méthode de Gauss (sur les formes quadratiques), trouver son nombre de racines distinctes et de racines réelles. Une deuxième vidéo pour l'étude d'un autre cas élémentaire : les racines sont toutes réelles mais non forcément distinctes, et la forme de Hankel est positive.

1.7.4 Les « Corona Sessions » de la prépa. Formes de Hankel 3/7

On propose ici une série de vidéos qui expliquent progressivement les formes de Hankel. L'idée est de partir d'un polynôme réel et, juste à l'aide d'identités de Newton et de méthode de Gauss (sur les formes quadratiques), trouver son nombre de racines distinctes et de racines réelles. Une troisième vidéo pour trouver la matrice de la forme de Hankel.

1.7.5 Les « Corona Sessions » de la prépa. Formes de Hankel 4/7

On propose ici une série de vidéos qui expliquent progressivement les formes de Hankel. L'idée est de partir d'un polynôme réel et, juste à l'aide d'identités de Newton et de méthode de Gauss (sur les formes quadratiques), trouver son nombre de racines distinctes et de racines réelles. La vidéo numéro 4 propose un exemple de calcul de forme de Hankel pour un polynôme réel de degré 2. Cette fois-ci, les nombres $alpha_i$ ne sont plus forcément ni distincts ni réels, mais s'il ne sont pas réels, ils seront conjugués.

1.7.6 Les « Corona Sessions » de la prépa. Formes de Hankel 5/7

On propose ici une série de vidéos qui expliquent progressivement les formes de Hankel. L'idée est de partir d'un polynôme réel et, juste à l'aide d'identités de Newton et de méthode de Gauss (sur les formes quadratiques), trouver son nombre de racines distinctes et de racines réelles. On va ici enfin (il était temps!) définir la forme de Hankel associée à un polynôme réel en toute généralité.

1.7.7 Les « Corona Sessions » de la prépa. Formes de Hankel 6/7

On propose ici une série de vidéos qui expliquent progressivement les formes de Hankel. L'idée est de partir d'un polynôme réel et, juste à l'aide d'identités de Newton et de méthode de Gauss (sur les formes quadratiques), trouver son nombre de racines distinctes et de racines réelles. On veut dans cette vidéo calculer la signature de la forme de Hankel associée à un polynôme réel T.

1.7.8 Les « Corona Sessions » de la prépa. Formes de Hankel 7/7

On propose ici une série de vidéos qui expliquent progressivement les formes de Hankel. L'idée est de partir d'un polynôme réel et, juste à l'aide d'identités de Newton et de méthode de Gauss (sur les formes quadratiques), trouver son nombre de racines distinctes et de racines réelles. On prouve le théorème de Hankel : la signature de la forme de Hankel d'un polynôme réel T « voit » son nombre de recines réelles, et son nombre de racines distinctes.

1.7.9 Les formes de Hankel (à leur état naturel)

Voici une présentation des formes de Hankel (associée à un polynôme P réel) vue dans leur élément naturel, c'est-à-dire, sur un espace de polynôme réel. Dans un premier temps, nous présentons le cas où le polynôme P est scindé sur $\mathbb{R}$.

1.7.10 Les formes de Hankel au naturel - 2

Voici une présentation des formes de Hankel (associée à un polynôme P réel) vue dans leur élément naturel, c'est-à-dire, sur un espace de polynôme réel. Nous présentons maintenant le cas général.

1.7.11 Représentation d'entiers par une forme quadratique - somme de carrés-1

Dans cette première vidéo, nous allons parler des entiers qui se réalisent comme sommes de deux carrés. Mais plus généralement, nous allons voir quels sont les entiers qui s'écrivent sous la forme $x^2 + dy^2$, avec x, y entiers, avec $d = 1,\ 2,\ 3, 5$. Nous allons voir que le cas $d = 5$ diffère des trois premier cas.

1.7.12 Représentation d'entiers par une forme quadratique - congruences - 2

On vient de voir empiriquement certaines relations entre la réalisation d'un entier p premier par une forme quadratique x^2+dy^2 (pour $d = 1, 2, 3, 5$) et certaines congruence de p. Nous montrons l'implication (facile) dans un premier temps.

1.7.13 Représentation d'entiers par une forme quadratique - Factorialité - 3

On a vu que la représentation d'entiers de la forme $m = x^2 + dy^2$, impliquaient certaines congruences de p. On montre dans les cas factoriels une réciproque. Les cas $d = 1$ ou 2 se font sans trop de difficulté, mais le cas $d = 3$ résiste un peu pour finalement céder. Pour le cas $d = 5$, il faudra tout reprendre à zéro !

1.7.14 Représentation d'entiers par une forme quadratique - FQ binaires - 4

Il faut se rendre à l'évidence que la factorialité ne sera pas toujours là pour nous venir en aide. Gauss, dans ses disquisitiones, propose une autre méthode, que nous exposons ici sur l'exemple $d = 5$, et qui passe par les classes de congruences de formes quadratiques sur $\mathbb{Z}^2$.

1.7.15 Représentation d'entiers par une forme quadratique - 5

On a vu dans la vidéo précédente que la réciproque qui consiste à partir de p premier congru à 1 ou 9 modulo 20 implique que p est représenté par $x^2 + 5y^2$ demande une connaissance sérieuse des classes de congruences de formes quadratiques sur $\mathbb{Z}$. C'est un petit résultat de finitude qui va nous permettre cette classification. On prouve alors la réciproque, mais on n'est pas au bout de nos surprises !

1.7.16 Représentation d'entiers par une forme quadratique - La trilogie-6

Une dernière vidéo sur les représentations d'entiers, où l'on explore la théorie des formes quadratiques binaires, leur lien avec les classes de conjugaison, les classes d'idéaux, et, sans vouloir faire d'idéologie en ce 14 juillet, un petit hommage à 350 polytechniciens qui rendent hommage à cet anniversaire de la révolution...

1.7.17 Forme quadratique sur l'espace des matrices carrées

Un petit exercice autour d'**une forme quadratique intrigante sur l'espace $\mathbf{M_n(K)}$.** En effet, elle est **définie par un coefficient du polynôme caractéristique de la matrice** (celui en X^{n-2}). Une fois rapportée à la forme trace, on répond à toutes les questions classiques du genre (non dégénérescence, signature sur $\mathbb{R}$).

1.7.18 Tout tétraèdre est régulier (en toute dimension) !

On montre ici que pour tout triangle non plat du plan, il existe un unique (à scalaire positif près) produit scalaire qui le rende équilatéral. On continue ensuite cette histoire en dimension 3 où l'on montre que tout tétraèdre (dont trois arêtes forment une base) est régulier. On finit par une généralisation en toute dimension. Mais au fait, qu'est-ce qu'un polyèdre régulier en toute dimension ? On fera un détour autour de cette question afin d'en expliquer les subtilités.

1.7.19 Formes quadratiques sur le corps des rationnels par Adem Zeghib

Adem nous propose une recherche guidée vers la question d'existence (ou non) de points rationnels solutions de l'équation $q(x) = 1$, où q est une forme quadratique définie positive à coefficients entiers. On va voir tout d'abord que l'existence d'un seul point rationnel implique toute une « sphère de points », puis, à l'aide de contre - exemples choisis, que cette existence n'est pas acquise en petite dimension.

1.8 Bouquet de géométries (48)

1.8.1 Le théorème de Thébault (quadrilatères et réduction)

Plusieurs thèmes en fusion dans ce petit exercice de géométrie faisant référence au théorème de Thébault, que l'on peut trouver dans Nouvelles Histoires Hédonistes de Groupes et de Géométries Tome 2 XIII-E.49. Calcul complexe, quadrilatères... mais un dictionnaire entre quadrilatères classiques et sous-espaces stables par la matrice compagnon de $X^4 - 1$. On en profite pour faire une petite publicité pour la théorie des représentations.

1.8.2 Une bonne tranche de cône (les coniques)

On va montrer grâce au théorème de Sylvester que toute conique non dégénérée provient d'une « tranche » d'un même cône appelé cône d'Apollonius. On ne va pas s'arrêter là et on va continuer notre investigation à d'autres dimensions.

1.8.3 Le cercle des neuf points par le calcul complexe (et en neuf minutes !)

La preuve du cercle des neuf points en neuf minutes ? C'est possible avec le calcul complexe. On commencera tout de même par une présentation des outils du calcul complexe au service de la géométrie euclidienne.

1.8.4 Utilisation de la réduction en géométrie affine - un exemple

La droite de Newton fournit un exercice classique qui peut se résoudre de plusieurs manières. Mais celle que nous proposons utilise les liens indispensables qui autorise la théorie de la réduction à venir nous sauver des problèmes de l'affine.

1.8.5 Quadrilatères et réduction des endomorphismes

Plusieurs thèmes en fusion dans ce petit exercice de géométrie faisant référence au théorème de Thébault, que l'on peut trouver dans Nouvelles Histoires Hédonistes de Groupes et de Géométries Tome 2 XIII-E.49. Calcul complexe, quadrilatères... mais un dictionnaire entre quadrilatères classiques et sous-espaces stables par la matrice compagnon de $X^4 - 1$. On en profite pour faire une petite publicité pour la théorie des représentations.

1.8.6 Les tutos géométriques du Père Castor : Géométrie affine euclidienne 4

Voici un exercice classique à l'oral durant une leçon sur les isométries du plan et de l'espace : la construction des éléments caractéristiques d'une symétrie glissée composée de trois symétries orthogonales par rapport à trois axes du plan euclidien. Présenté par Antoine.

1.8.7 Les tutos géométriques du Père Castor : Puissance d'un point, axe radical

Notre ami Antoine va nous montrer comment calculer la puissance d'un point par rapport à un cercle, tracer une tangente à un cercle à partir d'un point et trouver, en trois coups de compas, l'axe radical de deux cercles, c'est-à-dire le lieu des points qui ont même puissance par rapport à deux cercles fixés

1.8.8 Les tutos géométriques du Père Castor : droites tangentes à deux cercles données

Comment placer deux droites tangentes à deux cercles donnés ? On va vous montrer que c'est très simple, et, comme on pourrait s'en douter, ce n'est pas sans rapport avec l'axe radical de deux cercles.

1.8.9 Les coniques. Un exercice képlerien (qui plaira !)

Voici un petit exercice de géométrie plane, qui fait d'autant plus planer que l'on peut l'imaginer se réaliser dans le macrocosme du système solaire. A partir d'un énoncé simple, on voit apparaître un conique dans sa description bifocale. On finit sur un petit fichier gif concocté par Jérôme Germoni.

Merci à mon ami Bruno C. pour la réf. Cours de mathématiques spéciales, tome 5 : Arcs et nappes de Bernard Gostiaux

1.8.10 Un exercice sur les coordonnées barycentriques d'un triangle

On présente une fonction du plan affine qui s'exprime en termes de coordonnées barycentriques à partir de trois points d'un triangle, et on cherche l'image du triangle de points milieux. Je vous donne en mille de l'objet image que l'on va rencontrer...

1.8.11 Le groupe des isométries du tétraèdre agit sur ses sommets

Un des points clef de l'isomorphisme entre le groupe des isométries du tétraèdre régulier et le groupe S_4 réside dans le fait que ce groupe permute les sommets du tétraèdre. Valérie regarde ce point dans tous ses détails.

1.8.12 Composée d'isométries planes - 1

Un petit compte-rendu (debriefing, ça parle plus peut-être ?) sur la composée d'isométries planes.

1.8.13 Composée d'isométries planes - 2

Quelques petits exercices de construction d'éléments caractéristiques d'isométries obtenues par composée de deux isométries. L'histoire de vérifier que la vidéo 1 a été bien digérée.

1.8.14 Exercices de confinement : homographies

Un petit exercice de transformation homographique dans le style de la partie I de l'épreuve EP1 de l'agrégation interne 2017. On montre que la transformation de Cayley envoie la droite réelle sur le cercle unité. On montre ensuite que cette transformation envoie le demi-plan de Poincaré sur le disque ouvert unité, par deux méthodes, une calculatoire, et l'autre topologique.

1.8.15 Les « Corona Sessions » de la prépa. Lyon - Ellipse de Steiner 1/6

On s'intéresse en 6 vidéos à l'ellipse de Steiner associée à un triangle. Plusieurs aspects seront étudiés autour de cette ellipse : géométrie, calcul complexe, groupes de transformations, relations coefficients-racines, équations de coniques... et le chat Gaston. Bref, plein de choses qui en effraient plus d'un, mais qui ronronnent tranquille quand on les a adoptées.

1.8.16 Les « Corona Sessions » de la prépa. Lyon - Ellipse de Steiner 2/6

Après avoir montré l'existence de l'ellipse de Steiner d'un triangle, on en montre l'unicité. Encore une fois, les groupes de transformations nous permettent de nous ramener à une forme plus sympathique.

1.8.17 Les « Corona Sessions » de la prépa. Lyon - Ellipse de Steiner 3/6

On aborde le problème des foyers de l'ellipse de Steiner. Pour l'instant, on ne fait qu'évoquer Gauss-Lucas et montrer que seul le groupe des isométries peut nous apporter quelque chose. Peu, mais ce sera suffisant pour démarrer.

1.8.18 Les « Corona Sessions » de la prépa. Ellipse de Steiner 4/6

Maintenant que l'ellipse de Steiner a été placée dans le plan complexe, axée sur la droite réelle et centrée en 0, on attaque la stratégie de calcul, basée sur la recherche de l'équation de l'ellipse à partir d'une équation de « cercle de Steiner » pour le triangle des racines cubiques de l'unité. On introduit sous forme complexe une transformation affine.

1.8.19 Les « Corona Sessions » de la prépa. Lyon - Ellipse de Steiner 5/6

On est en mesure de calculer l'équation de l'ellipse sous une forme dont on sait déduire les foyers.

1.8.20 Les « Corona Sessions » de la prépa. Lyon - Ellipse de Steiner 6/6

A l'aide l'équation de l'ellipse de Steiner, on en calcule les foyers et on vérifie à l'aide de relations coefficients-racines qu'ils coïncident avec les racines du polynôme dérivé du triangle de départ.

1.8.21 Les « Corona Sessions » de la prépa. Droites et cercles 1/5

Les droites et cercles du plan sont étudiées à l'aide du calcul complexe, du groupe des homographies... et du birapport. Dans une première vidéo, on introduit, à l'aide des complexes, deux caractérisations de la cocyclicité (ou alignement) de quatre points. Une en termes d'arguments et l'autre de modules.

1.8.22 Les « Corona Sessions » de la prépa. Lyon - Droites et cercles 2/5

On présente maintenant le groupe des homographies. Il s'agit d'un groupe de transformations qui contient les translations, les similitudes directes et qui va préserver les cercles et droites. « Oui, mais quand ? » comme dit mon collègue préféré. Et bien quand vous serez prêts à le regarder en face !

1.8.23 Les « Corona Sessions » de la prépa. Droites et cercles 3/5

On étudie une chaîne d'actions de groupes emboîtés sur le plan complexe (prolongé par l'infini). Les translations amènent à la notion de bipoints équipollents, les similitudes directes à celle de triangles semblables et enfin les homographies à celle de quadruplets de points ayant même birapport. Lorsque ce dernier est réel, les quatre points sont cocycliques ou alignés.

1.8.24 Les « Corona Sessions » de la prépa. Lyon - Droites et cercles 4/5

Dans cette vidéo, on montre que le groupe des homographies agit de façon transitive sur l'ensemble des « cercles et droite ».

1.8.25 Les « Corona Sessions » de la prépa. Lyon - Droites et cercles 5/5

On montre ici l'inégalité de Ptolémée et son cas d'égalité, qui caractérise les quadruplets de points inscriptibles sur un cercle à l'aide des distances entre ces points. Encore une fois, le birapport est en première ligne.

1.8.26 Géométrie borderline à l'agrégation

Cercles tangents

On étudie un petit exercice sur les cercles tangents. But du jeu : trouver trois cercles distincts du plan et 8 cercles tangents à ces trois cercles. Ce petit exercice qui semble anodin ouvre un champ vers la géométrie anallagmatique (que nous rappelons à l'occasion) et même (mais on ne visitera pas cet aspect des choses) aux arcanes profonds de la théorie d'intersection et de l'édifiant théorème de Chasles sur les 3264 coniques tangentes à 5 coniques données.

Cercles tangents-2

On vient de résoudre le problème de trouver trois « cercles-droites » possédant 8 cercles tangents. Maintenant, il est temps de transformer les (deux) droites en cercles et le cercle en un autre cercle. On le fait en utilisant des translations et des inversions. A la suite de quoi, on discute de choses afférentes cachées derrière ce problème, comme le problème de la triple transitivité du groupe engendré par les inversions (homographies et antihomographies) sur les « droites ou cercles » ainsi que la théorie d'intersection, qui sera à peine évoquée.

Alternative de Steiner (Cercles tangents-3)

On présente sous forme d'exercice corrigé (la correction dans une prochaine vidéo) l'alternative de Steiner. Encore une fois, les groupes de transformations et leurs invariants jouent un rôle central.

Alternative de Steiner (Cercles tangents-4)

On résout l'exercice sur l'alternative de Steiner. Il suffisait de se ramener, par homographie, à deux cercles concentriques, et le problème se résout miraculeusement à l'aide de tout petits calculs.

Géométrie des cercles (ou droites) - Pour débuter avec la géométrie analagmatique - 1

On va, à partir de ce que nous savons tous sur les cercles et droites, créer un lien entre leur géométrie et celle de l'espace de Lorentz, c'est-à-dire, l'espace $\mathbb{R}^4$ muni d'une forme quadratique de signature $(3, 1)$. On écrit ici tous les résultats dans un tableau à double entrée pour cette belle correspondance, et on fera les preuves dans une prochaine vidéo.

Géométrie des cercles (ou droites) - Pour débuter avec la géométrie analagmatique - 2

On a donné, dans une première vidéo, un tableau qui mettait en relation des cercles du plan euclidien et des droites de l'espace $\mathbb{R}^4$ muni de la forme de Lorentz. Dans cette vidéo, on passe aux preuves, que l'on peut retrouver dans NH2G2, XI-3. 3. 8.

Géométrie des cercles (ou droites) - Pour débuter avec la géométrie analagmatique - 3

On commence à minutieusement mettre en place une correspondance entre droites et cercles du plan complexe, d'une part, et droites de l'espace $\mathbb{R}^4$. On peut, par section hyperplane, voir tout cela assez agréablement dans $\mathbb{R}^3$ euclidien muni de sa boule unité.

Géométrie des cercles (ou droites) - Pour débuter avec la géométrie analagmatique - 4

Par cette correspondance que nous avons construite en transformant un cercle en une « droite de l'espace de Lorentz $\mathbb{R}^4$ » grâce à son équation, on utilise Sylvester pour classifier les faisceaux de cercles et les faisceaux orthogonaux.

Géométrie des cercles (ou droites) - Pour débuter avec la géométrie analagmatique - 5

On a pour l'instant un joli modèle pour l'étude des cercles, qui sont représentés comme des points d'un espace projectif de dimension 3. Dans cet espace, nous allons voir que les points d'un cercle donné se voient sur une sphère, puis, par projection stéréographique, on va retrouver le cercle dans la géométrie de $\mathbb{R}^4$.

Géométrie des cercles (ou droites) - Pour débuter avec la géométrie analagmatique - 6

Dans cette vidéo, on introduit l'action de $SL_2(\mathbb{C})$ sur les cercles par homographie. Nous l'avons déjà dans une playlist, mais cette fois-ci, l'originalité vient du fait que cette action provient de l'action par congruence sur les formes hermitiennes, et donc leurs cônes isotropes. Nous sommes à deux doigts de conclure à une des plus belles correspondances de la géométrie, qui fait toute la richesse de la géométrie analagmatique.

Géométrie des cercles (ou droites) - Pour débuter avec la géométrie anallagmatique - 7

On prouve un isomorphisme entre les groupes simples $PSL_2(\mathbb{C})$ et $PSO(q)$, qui sera ensuite prolongé par un isomorphisme un peu plus complet. On finit alors sur un tableau de correspondance entre deux versions de la même géométrie, dite anallagmatique, en indiquant comment ces deux versions se complètent pour créer une géométrie puissante.

Empilement de sphères 1

Dans un style récréatif, nous allons parler de tentatives d'empiler des sphères les unes sur les autres en minimisant les pertes d'espace. Il s'agit là d'une problématique qui remonte (au moins) à Kepler en passant par Minkowski et, bien sûr, mon épicier. On propose différentes façons d'empiler des sphères dans un espace et on fait quelques calculs de densité.

Empilement de sphères 2

On propose maintenant d'interpréter les densités d'empilements de sphères. En dimension 1 (une évidence), en dimension deux (où on a comparé deux options). Jusque là, les mathématiciens ont su prouver qu'il s'agissait des empilements les plus efficaces (même si on ne décide pas de se limiter aux empilements basés sur un réseau). On va alors comparer deux façons d'empiler des oranges, la façon dite de l'épicier, et une autre qui semble plus logique au mathématicien. On constate la même densité, et on en donnera deux petites explications, une géométrique (un héxagone inscrit dans le cube, plus précisément dans un cuboctaèdre) et une, plus algébrique, par les deux matrices de Gram des réseaux qui se trouvent être $\mathrm{GL}_3(\mathbb{Z})$ -congruentes.

Empilement de sphères 3

On termine cette petite fenêtre sur les empilements de sphères avec le cas des dimensions supérieures,. On y rencontrera, en dimension 4, l'icositétrachore, qui optimise le placement d'hypersphères sur un réseau, puis, en dimension 8 le système de racines E_8 qui a fait les beaux jours de la jeune chercheuse Maryna Viazovska.

Structure de groupe sur une conique 1/9

Voici une petite série de vidéos où l'on présente une construction de groupe sur les coniques. Il s'agit d'une construction qui fait le point sur des propriétés géométriques des coniques bien cônues depuis Pascal, et dont les applications à la cryptographie (que l'on effleurera seulement) sont apparues de façon relativement récente. Cette première vidéo est avant tout un teaser.

Structure de groupe sur une conique 2/9

Dans cette vidéo, on donne la construction générale pour la structure de groupe sur une conique non dégénérée. On montre que l'on a bien un groupe dans trois cas particuliers. Et ces groupes ne sont pas anodins. Il s'agit du groupe additif (pour la parabole), du groupe multiplicatif (pour l'hyperbole), et le groupe additif modulaire, comme les groupe des angles, (pour l'ellipse). Si on ajoute à cela que ces groupes géométriques sont à la fondation de la cryptographie actuelle, on se dit qu'il n'y a que les maths pour nous faire traverser, dans une logique implacable, l'histoire antique, notre monde actuel, et les souvenirs nostalgiques des premières opérations de notre enfance.

Structure de groupe sur une conique 3/9

Après avoir mis une opération sur une conique (munie d'un point), et après avoir montré que cette opération fournit une structure de groupe sur trois exemples représentatifs de la classification affine, on montre que la structure de groupe se transmet d'une conique à l'autre par une transformation affine. Et contre cette transmission, il n'y a ni masque, ni geste barrière !

Structure de groupe sur une conique 4/9

On attaque le théorème principal. Sur le fait que notre opération géométrique confère une structure de groupe qui caractérise le type affine de la conique. Au passage, on montre, à l'aide de changements de variables, le résultat souvent mal digéré sur la fameuse classification affine des coniques. Ce résultat sera parachevé dans une vidéo suivante.

Structure de groupe sur une conique 5/9

On finit ici la preuve du théorème de classification des coniques non dégénérées par les trois groupes classiques réels.

Structure de groupe sur une conique 6/9

On a montré le théorème de structure de groupe sur une conique, à l'aide d'un mélange de petit calculs dans trois cas simples et de groupes de transformations. On veut maintenant une preuve plus directe en travaillant sur la géométrie de la conique. L'associativité pose un petit problème, qui va être résolu grâce au théorème de l'hexagramme mystique de Pascal.

Structure de groupe sur une conique 7/9

On a eu besoin d'une version projective du théorème de l'hexagramme mystique de Pascal. Voici quelques notions de projectif pour mieux comprendre ce que veut dire « envoyer une droite (ou un point) à l'infini » dans les manipulations de géométrie (projective). On verra également que le projectif confond paraboles, ellipses et hyperboles, alors que l'affine les distingue.

Les « Corona Sessions » de la prépa. Structure de groupe sur une conique 8/9

On pensait arrêter là, mais l'arithmétique a mis le pied dans la porte, et on est repartis sur deux autres vidéos. Ici, on s'intéresse toujours à la structure de groupe sur une conique, mais cette fois-ci sous l'angle de l'équation diophantienne dite de Pell-Fermat. On verra trois groupes isomorphes : la conique de l'ensemble des solutions entières de l'équation, l'ensemble des unités positives d'un anneau quadratique réel, et tout bonnement, le groupe monogène des entiers.

Les « Corona Sessions » de la prépa. Structure de groupe sur une conique 9/9

Dernier volet de la série où l'on montre (en mode DSK) comment les coniques, en leur ajoutant une droite, sont des dégénérescences d'une famille de courbes elliptiques. On finit sur des explications (à détailler avec de bonnes références !) sur les applications de ces dernières à la cryptanalyse et à la cryptographie.

Utilisation de l'arithmétique dans les polygones (un exercice)

Tout le monde a remarqué que la longueur des côtés d'un rectangle est périodique de période 2 (Longueur-Largeur-Longueur-Largeur). Et bien cette propriété se généralise avec les longueurs d'un p^n-gone dont les angles sont réguliers... Arriverez-vous à le montrer ?

La formule de Héron en dimension n (par le déterminant de Cayley-Menger)

On donne une version déterminante de la formule de Héron, qui fournit l'aire d'un triangle en fonction de la longueur de ses arêtes. L'énorme avantage de cette nouvelle version et d'être généralisable à n'importe quel simplexe en toute dimension. Cela permettra un rappel non inutile des vertus du déterminant pour calculer des volumes :-)

Qui c'est le plus fort, l'hyperbole ou l'ellipse ?

Comment comparer l'hyperbole et l'ellipse ? En mettant les deux sur le ring !

Pourquoi une isométrie est-elle une application affine ?

C'est un résultat très connu qui nous dit que si une application d'un espace euclidien vers lui-même respecte la norme, alors elle est automatiquement linéaire. Voici une preuve claire de ce résultat.

Que nul n'entre ici s'il n'a point d'invariant

Une petite vidéo pour illustrer comment les invariants fleurissent en géométrie(s). Une idée fructueuse consiste à faire agir dans le contexte d'une géométrie un groupe G sur un ensemble X et de voir quand le groupe "décroche" en terme de n-transitivité, ie G agit n-transitivement sur X, mais pas n+1-transitivement. A ce moment, on est prêt à récupérer le précieux invariant ! On montre cette idée unifiante sur l'exemple, des angles, angles orientés, rapports, birapport, invariant anallagmatique, et même sur la réduite de Jordan !!!

Napoléon trivialisé par Maître Yoda ! Régularisation d'un n-gone

Voici un magnifique problème proposé par Jean-Jacques Juré. Le théorème de Napoleon permet de régulariser un triangle. Nous allons voir qu'il est possible également de régulariser un n-gone pour tout n, ce que l on appellera le théorème de Napolygone (merci mpc formation) ! ! ! Voici un problème qui ne manquera pas de séduire à la fois ceux qui aiment la géométrie plane que ceux qui aiment la réduction, l'analyse spectrale, et toutes leurs interférences !

1.9 Un epsilon d'analyse (23)

1.9.1 Petit exercice sur les équations différentielles linéaires

Un exercice donné à l'agrégation interne sur une leçon qui concernait les équations différentielles linéaires à coefficients constants.

1.9.2 L'intégrale de Dirichlet par Riri

Haut les coeurs ! Riri l'intrépide nous présente un développement sur l'intégrale de Dirichlet, avec un méthode simple et élégante.

Attention, petite coquille à la fin repérée par $Toto^2$. Il faut lire intégrale de 0 à l'infini au lieu de l'intégrale de 0 à $pi/2$. Toujours dans les remarques de $Toto^2$, l'intégrale J_n peut être vue comme le noyau de Dirichlet. On peut donc imaginer que l'intégrale de Dirichlet est plutôt une conséquence directe, attribuée à Dirichlet, de son noyau ! C'est-à-dire que dans l'histoire telle qu'elle s'est déroulée va dans le sens inverse du développement : -)

1.9.3 Erreur dans l'approximation par la méthode de quadrature

La méthode de quadrature de Gauss est une méthode qui force le respect ainsi que la porte vers la théorie des polynômes orthogonaux. Après avoir survolé les résultats principaux que l'on peut trouver dans Carnet de Voyage en Analystan ainsi que dans la vidéo de Caroline `https://youtu.be/d7qu0RVGSdY` on donnera une estimation de l'erreur commise par cette approche. On finira par une application pour une approximation du nombre pi.

1.9.4 Méthode de quadrature de Gauss par Caroline

Voir Carnet de Voyage en Analystan (et particulièrement dans la nouvelle édition qui vient de sortir !) La méthode de quadrature de Gauss donne des nombres réels permettant d'intégrer un polynôme sur un intervalle à partir d'une combinaison linéaire de ce polynôme en ces réels. Le plus étonnant dans cette histoire est que l'on n'a besoin que de n réels pour un polynôme de degré $2n-1$. C'est ce que va nous raconter Caroline. Il s'en suivra l'inévitable série de questions de jury !

1.9.5 TOUT sur les nombres de Bernoulli !

Vidéo 1 : On présente ici les nombres et les polynômes de Jacques Bernoulli. Ces nombres se retrouvent miraculeusement à la fois en algèbre, en combinatoire, en théorie des nombres, en arithmétique, mais aussi en analyse, en théorie de Fourier, en topologie, K-théorie, et il se rencontre de façon naturelle en algèbre non commutative. On va introduire ces nombres par analyse-synthèse par la recherche de polynômes permettant de calculer des sommes de Newton.

Vidéo 2 : Maintenant que l'on a appris à écrire sans faute le mot « Bernoulli » dans la première vidéo (entre autres, grâce au pense-bête « Bernoulli n'est pas une nouille »), on prouve une formule non totalement triviale qui permet de calculer explicitement les fascinants nombres de Bernoulli.

La preuve passe par la formule donnant le nombre $s_{n,m}$ de surjections d'un ensemble à n éléments vers un ensemble à m éléments (via la formule du crible), puis un résultat surprenant (et intéressant en soi) qui prouve que $s_{n,m}$ est le coefficient de la base canonique des polynômes dans la base des polynômes de Hilbert !

Vidéo 3 : On établit, à l'aide de la formule de Dirichlet sur les séries de Fourier, un lien entre les nombres de Bernoulli et la fonction zeta de Riemann.

Vidéo 4 : Mais pourquoi les nombres de Bernoulli apparaissent-ils ainsi, comme en génération spontanée, dans divers domaines des mathématiques ? Finalement, c'est peut-être cette famille $B_n(t)/n!$ qui s'apparente à la famille $x^n/n!$ dans son comportement vis-à-vis de la dérivée... Il est alors normal que les nombres de Bernoulli se retrouvent dans les développements limités de la famille des exponentielles. On donne ici le développement de xcot (x) en 0. On saluera en passant les fécondes méthodes de déformation en analyse.

1.9.6 Exercices de confinement : normes sur $\mathbb{R}[X]$-1

On commence une série de petits exercices présentant des contre - exemples sur les normes non équivalentes lorsque les espaces vectoriels sont de dimension infinie.

1.9.7 Exercices de confinement : normes sur $\mathbb{R}[X]$-2

On continue avec un exercice qui relie certaines normes sur $\mathbb{R}[X]$ à des « compacts infinis » de $\mathbb{R}$. Notons que « compact infini » est une notion essentielle dans les problèmes de prolongements analytiques en analyse complexe.

1.9.8 Exercices de confinement : normes sur $\mathbb{R}[X]$-3

On attaque un petit dernier sur les normes de $\mathbb{R}[X]$. On introduit une norme un peu farfelue sur $\mathbb{R}[X]$ et on montre que l'espace $\mathbb{R}[X]$ n'est pas complet pour cette norme. Au final, on voit que c'est peine perdue *puisqu'un* espace à base dénombrable sur $\mathbb{R}$ ne peut pas être complet pour aucune norme.

1.9.9 Comportement asymptotique des suites récurrentes

On cherche à comprendre les équivalents autour d'un point (y compris l'infini) à une suite récurrente de type $u_{n+1} = f(u_n)$. On présente ensuite un classique. La suite $u_{n+1} = \sin(u_n)$ avec u_0 assez proche de 0 tend vers 0. On voit, comme dans la vidéo précédente (dont celle-ci est une illustration), que u_n est équivalent à sqrt $(3/n)$ en l'infini. On cherche ensuite un second terme à son développement asymptotique.

1.9.10 Combinatoire et placements de table

Une formule certainement utile pour les fêtes de fin d'années : de combien de façons peut-on placer n couples autour d'une table de sorte que chaque couple soit séparé. Et nous voici en route pour une aventure festive (et mathématique !)

1.9.11 La suite $u_{n+1} = \sin(u_n)$ et son comportement asymptotique

Riri, qui a le sens de la fête, et celui des paillettes, s'est mis sur son 31 (!) pour nous présenter le comportement asymptotique de la suite récurrente associée à la fonction sinus. Un développement issu de Carnet de Voyage en Analystan (et non pas algébrie...)

A ce propos, comme le fait remarquer Alexis Roussel, attention à la fin où l équivalent doit être remplacé par une écriture avec des o de Landau. Plus précisément, on doit partir de

$u_n^{-2} - u_0^{-2} - n/3 = log(n)/5 + o\,(\mathrm{Log}\,(n))$

Cette vidéo sera donc instructive à plus d'un titre sur les avantages et les dangers de l'utilisation des équivalents. Il faut savoir les utiliser à bon escient, et savoir remplacer f equivalent a g par $f = g + o(g)$ quand cela est nécessaire.

1.9.12 Vitesse de convergence d'une suite récurrente (et méthode d'Archimède)

On part d'une situation classique où une suite récurrente (u_n) donnée par une fonction converge vers un point fixe attractif r et on voudrait savoir si la suite $r - u_n$ est équivalente à une suite géométrique. Ceci nous amène à un exemple deux fois millénaire, avec la méthode d'Archimède pour approcher le nombre *pi*... et comme on n'est jamais à court d'histoires, on parlera du jeune Grothendieck.

1.9.13 Erreurs dans les calculs d'intégrales - 2

Nous parlons ici des différentes méthodes pour les calculs d'intégrales (rectangle, trapèze, méthode de Simpson, et une introduction à la méthode de quadrature de Gauss). Voici cette fois-ci le pendant analytique de la première vidéo. On calcule, à l'aide de l'inégalité des accroissement finis, un encadrement des erreurs que l'on fait en appliquant ces méthodes à une fonction « suffisamment dérivable » sur un intervalle $[a, b]$.

1.9.14 Un exercice sur Taylor-Lagrange

Un petit exercice parfait pour une kholle en prépa : -) qui fournit un critère par la positivité pour que la série de Taylor d'une fonction converge en un point. On donnera deux preuves, une, avec la formule de Taylor-Lagrange, et l'autre en utilisant la version avec reste intégral.

1.9.15 Utilisation des fractions rationnelles (dérivées de l'arctangente)

Il faut souvent se gratter la tête pour trouver des exercices ou des exemples d'utilisation dans les énoncés d'oraux de l'agrégation interne. En particulier pour l'utilisation de fractions rationnelles ! Voici un petit exemple d'application...

1.9.16 Problème de la corde universelle (problème d'Olympiades)

Un petit problème de type « olympiades » que m'a indiqué Roger Mansuy, et qui demande juste un peu de réflexion et de TVI (théorème des valeurs intermédiaires). La partie positive du problème aboutit aux théorème de la corde universelle, et l'autre partie nous amènera à un contre - exemple bougrement tordu, mais sacrément intelligent.

1.9.17 Pourquoi une fonction injective continue sur un intervalle est-elle strictement monotone ?

On donne trois preuves pour cet énoncé. Une fausse (ou disons trop imprécise), une pour le niveau licence, et enfin une, assez séduisante, mais qui demande quelques bases de topologie de L3.

1.9.18 Primitivable implique continue (ou bien) ?

On sait depuis longtemps qu'une fonction continue sur un intervalle est possède une primitive. Mais est-ce bien nécessaire ? On va commencer par donner un contre - exemple (classique) d'une fonction primitivable non continue. Mais si admettre une primitive n'implique pas forcément la continuité, le théorème des accroissements finis prouve qu'il s'agit d'une fonction vérifiant le théorème des valeurs intermédiaires, que l'on appelle également fonction de Darboux. Encore une fois, la réciproque est fausse et on va montrer qu'une fonction de Darboux n'est pas nécessairement primitivable.

1.9.19 Normes, boules et stricte convexité 1

On étudie le problème de stricte convexité des normes sur un espace vectoriel. On montre que l'axiome de stricte convexité correspond à un problème de stricte convexité des boules. On fournit ensuite un petit outillage pour montrer qu'une norme est strictement convexe.

1.9.20 Normes, boules et stricte convexité 2

Nous étudions la distance d'un point à un fermé F. On commence dans le cadre où F est un hyperplan affine, une sphère, un fermé quelconque, puis, un fermé convexe dans le cadre d'une norme strictement convexe.

1.9.21 Normes, boules et stricte convexité 3

On peut maintenant dans ce troisième volet prouver un théorème de séparation qui dit que si F est un fermé convexe et M un point hors de F, on peut trouver un hyperplan H qui les sépare, c'est-à-dire, un hyperplan qui définit deux demi-espaces ouverts H^+ et H^- tels que x soit dans H^+ et F inclus dans H^-.

1.9.22 Comment j'ai aimé la convexité... (un mini-cours)

On propose ici un cours a minima sur la convexité. Il s'agit là d'une théorie plutôt mal digérée par les étudiants (et j'en ai été le premier à en souffrir) dont on va essayer d'extraire tous les arcanes. Pour aller au plus pressé, nous introduisons la notion de projection sur un compact convexe (que l'on retrouve dans pas mal d'épreuves de concours, dont le fameux EP2-2025 de l'agrégation interne) puis, la notion d'hyperplan séparateur. Ce dernier est un sésame à pas mal de problèmes sur les convexes. Mais le plus merveilleux arrive au moment de l'étude des convexes compacts avec 0 dans leur intérieurs qui jouissent d'une belle (et rare !) dualité que l'on ne se lassera pas de regarder sous des formes diverses !

1.9.23 Normes vs CCS (Corps convexes symétriques)

On montre que la donnée d'une norme de $\mathbb{R}^n$ est équivalente à la donnée de sa boule fermée $B(0,1)$. Mais que doit vérifier une partie de $\mathbb{R}^n$ pour être la boule d'une norme ? Tout est dans la notion de corps symétrique convexe qui va venir jouer le pendant géométrique de séparable-homogène-inégalité triangulaire de la norme !

1.9.24 Le cercle d'incertitude d'une série entière

On donne, à partir d'exemples et de conjectures, de bonnes raisons d'appeler la frontière du disque de convergence d'une série entière, le « cercle d'incertitude » (des poètes disparus).

1.9.25 Complétion p-adique ou réelle ? Le théorème d'Ostrowski

Comment compléter le corps Q des rationnels ? Dit autrement, quelle analyse au menu ? C'est le théorème d'Ostrowski, que l'on prouvera dans cette vidéo, qui va nous dire que seules deux types de complétions sont possibles. On fera donc de l'analyse sur $\mathbb{R}$ ou sur $\mathbb{Q}_p$.

1.9.26 Distance de Hausdorff (et une surprise à la fin)

On montre qu'un espace métrique complet possède un espace métrique complet pour l'ensemble de ses compacts pour la métrique de Hausdorff. Une surprise à la fin !

1.9.27 Théorème de stabilité de Liapounov (équations différentielles non linéaires)

Voici un développement sur les équations différentielles non linéaires qui utilise la comparaison avec une équation différentielle linéaire. On trouve une condition pour obtenir une solution avec un point d'attraction à convergence exponentielle.

1.9.28 Critère de stabilité de Liapounov

Une matrice A de $\mathcal{M}_n(R)$ est dite stable si ses valeurs propres ont toutes une partie réelle strictement négative. On donne un critère de stabilité en terme de système linéaire. Au programme, réduction, exponentielle de matrices, systèmes linéaires, intégrales de matrices, et j'en passe.

1.9.29 Comportement lipschitzien du spectre (d'une matrice symétrique)

On sait (ou pas) que le rayon spectral d'une matrice symétrique définie positive est égal à sa norme subordonnée pour la norme quadratique. Les inégalités de Weyl nous permettent de voir que l'application qui, à une matrice symétrique réelle S, envoie la k-ième valeur propre de S (pour l'ordre naturel de $\mathbb{R}$), est 1-lipschtzienne. Au programme, thérème spectral, principe du min-max, inégalité de Weyl... Bref, on rentre dans la légende !

1.9.30 Réarrangements dans les Sobolev : le teaser par Tristan

Une visite surprise chez Tristan qui fait ses premiers pas dans le monde ardu de la thèse. Peut-être pour moi une des dernières chances avant décollage de comprendre ce qu'il fait : -).

En tout cas, la mission est accomplie parce que, sans préparation, Tristan raconte ses premières directions avec lucidité, passion et pédagogie.

PS : désolé pour le bruit des travaux sur le campus. Lyon peaufine son réseau de tramway. On supporte parce que c'est pour la bonne cause ! On pourra tout de même apprécier cette petite réverb' qui règne dans cette salle et donne cette impression de temps suspendu.

1.9.31 Espace complet de fonctions lipschitziennes

Un petit développement assez simple que l'on peut trouver dans Oraux-X ENS Analyse 3.

1.9.32 Un contre-exemple pour la convergence dominée et lemme de Fatou

Il est utile d'avoir dans sa musette des contre-exemples pour les théories que l'on utilise régulièrement. En voici un sur le théorème de convergence dominé ! On termine sur de petites considérations sur le lemme de Fatou.

1.9.33 Variations sur la série harmonique

On sait que la série harmonique (la somme des 1/n) diverge, mais que peut-on dire si on la somme sur un ensemble plus restreint ? Comme les nombres qui n'ont pas de 9 dans leur écriture décimale ? Ou les nombres qui ont "peu" de 9 dans leur écriture décimale ?

1.9.34 Principe du prolongement analytique et application

On prouve le principe du prolongement analytique pour les fonctions holomorphes sur un ouvert connexe U (donc analytiques sur U). On donne en exercice une petite application sympathique !

1.9.35 La preuve la plus courte pour C algébriquement clos ?

François, qui n'est plus à présenter sur cette chaîne, nous propose le "d'Alembert-Gauss-Express", peut-être une des preuves les plus courtes compte tenu du seul outil qu'elle utilise : une fonction continue sur un fermé borné de C est bornée et atteint ses bornes. Une preuve élémentaire en 9 minutes chrono, de ce théorème bien connu que j'aurais tendance à appeler le théorème légendaire de l'analyse plutôt que le théorème fondamental de l'algèbre...

1.9.36 Le théorème de stabilité de Liapounov

Le théorème de stabilité de Liapounov donne des conditions pour que, localement, les solutions de l'équation différentielle y'=f(y) se comporte "comme" l'équation linéaire z'=Az où A est la matrice de la différentielle en 0 de f. On peut en faire un joli développement avec un peu de réduction, de formes quadratiques et bien sûr, de calcul différentiel !

1.10 Probabilité et combinatoire (8)

1.10.1 Séries génératrices-mode d'emploi

Quelques petits exemples progressifs autour des séries génératrices dont le slogan pourrait être : « Si vous ne pouvez pas trouver un terme dans une suite, le mieux c'est de les compter tous ! »

1.10.2 Combinatoire sur le groupe des permutations

Deux petits exercices (en attendant d'en avoir deux plus gros) sur la moyenne du nombre de cycles (dans la décomposition en cycles à supports disjoints) et la moyenne du nombre d'inversions dans le groupe symétrique. Référence H2G2- tome 2 (2015) Chapitre IV.

1.10.3 Dés pipés et factorisation de polynômes

Deux dés sont numérotés de 1 à 6 et donc la somme des lancers des deux dés varie de 2 à 12. On veut savoir si l'on peut piper ces deux dés indépendamment de sorte que toutes les possibilités soient équiprobables. Bien sûr, le problème en cache un autre, plus général. Et on débouche sur un problème de factorisation de polynômes...

1.10.4 Question de jury- Dénombrement et polynômes (dés non pipés)

Voici une petite question à la fois jolie et instructive sur un lancer de dés non pipés ! Merci à Daniel Juteau pour le partage de son bel exercice. Et mention spéciale de l'humour mathématique à Riri qui dit n'avoir rien pipé ! `:-)`

1.10.5 Borel-Cantelli et les amis de la poésie !

On présente un exercice proposé par Guillaume Aubrun autour d'un poète prolifique qui veut relire toutes ses poésies. Cet exercice est une introduction au théorème de Borel-Cantelli.

1.10.6 L'urne de Polya (tirage avec renforcement)

On effectue un tirage successif avec remise, mais avec la particularité d'ajouter à l'urne un nombre fixé de boules de la dernière couleur tirée. On présente ici trois méthodes, sous les conseils avisés de Yan Doumerc (notre caution proba !), qui fournissent un joli florilège des outils à notre disposition en probas discrètes. Scoop ! Parmi ces outils figurent les actions de groupes !

Errata. Dans l epilogue, je voulais dire que les X_i suivent une. loi de Bernoulli mais leur somme S_n ne suit pas une loi binomiale.

1.10.7 Tirage de nombres premiers entre eux

On tire indépendamment deux nombres de 1 à n et on veut connaître la probabilité de tirer des nombres premiers entre eux lorsque n est grand. Dans ce développement que l'on peut trouver dans Carnet de Voyage en Analystan, on verra comment la fonction zeta débarque dans la théorie des nombres.

1.10.8 Tirage sans remise de n boules paires

Un petit exercice de probabilité qui permettra de tester nos formules sur la variance et la covariance ainsi que notre système D dans ce genre de situations.

Attention toutefois car les probas ne font pas partie de mes domaines de compétence! Yan Doumerc (que je remercie en passant) me fait remarquer à juste titre que la formulation « probabilité de X_i » n'est pas très heureuse, X_i étant une variable aléatoire et non un évènement. La confusion entre les deux est fréquente chez les étudiants et parmi les candidats à l'agrégation, elle est très préjudiciable. Je voulais bien sûr dire probabilité que $X_i = 1$.

1.10.9 Commutations dans le groupe des permutations

Un exercice finalement très simple une fois qu'on a compris la solution : -)) On cherche la probabilité que deux éléments commutent dans S_n, puis on veut montrer que cette probabilité tend vers 0 quand n tend vers l'infini.

1.10.10 Pour une combinatoire équitable

Une petite vidéo pour un plaidoyer en faveur d'une combinatoire durable et équitable, qui met en parallèle sous-structure et structure quotient (les deux piliers du temple de l'algèbre!), c'est-à-dire ici nombre de parties (coefficients binomiaux) et nombres de partitions, à k éléments. Le prétexte est alors de comprendre la variable qui, à une fonction de $[1,\ n]$ vers $[1, m]$, associe le cardinal de son image directe. Comme application, on traite deux problèmes : le problème des anniversaires, et les problème des vignettes de footballeurs (ou de pokemon, selon les goûts).

1.10.11 Le problème des chars d'assaut allemands

Un problème très jouable en développement qui couvre bien le programme de probabilités (Formules combinatoires, loi uniforme, inégalité de Markov, Bienaymé-Chebyshev, Théorème central limite) autour de la recherche (historique!) du nombre de chars que possédait l'Allemagne en 1942.

2 Annales

2.1 Conseils

2.1.1 Les écrits de l'externe pour l'agrégatif interne!

Une mise au point pour ceux qui veulent passer les écrits de l'externe avec bagage de l'interne.

2.2 Agrégation externe

2.2.1 Agrégation MG-2024 La fin de l'épreuve (II-D et III)

Toutes les bonnes choses ont une fin sauf $Wayne's$ World qui en a deux. On passe en mode avance rapide sur la fin du problème, mais sans toutefois en éluder les partie épineuses.

2.2.2 Agrégation MG-2024 Correction de la partie II-C

Une correction de la partie II-C de ce joli problème sur les sous-structures commutatives dans $\mathcal{M}_n(K)$. Les choses se simplifient maintenant qu'on a prouvé le plus lourd dans la partie II-B. But *don't* relax yet ! Car la question 17 est à la fois redoutable et plein de surprises !

Je donne dans la vidéo une preuve de 17b qui ne suis pas l'indication (décidément, je ne suis pas un suiveur : -). theob-yt me fait remarquer que l'idée était probablement de montrer que le sous-espace nilpotent maximal étant de dimension $b(n)$, et vu que $b(n) + 1 - n$ est strictement positif, il existe une matrice non nulle à la fois dans A et dans le sous-espace des matrices de première colonne nulle. C'est donc une matrice non inversible et non nulle.

2.2.3 Agrégation MG-2024 Correction de la partie II-A-B

Une correction de la partie II-A et B de ce joli problème sur les sous-structures commutatives dans $\mathcal{M}_n(K)$. On rentre ici dans la partie la plus difficile du problème avec en particulier une question 9c) manifestement fausse, une question 11a) difficile à rédiger et une question 13 élégante très élégante : -), mais qui pouvait donner du fil à retordre aux candidates et candidats. En même temps, on est dans des zones du problème où (si l'on a fait ce qui précède) on était tiré d'affaires !

2.2.4 Agrégation MG-2024 Correction de la partie I

Une correction de la partie I de ce joli problème sur les sous-structures commutatives dans $\mathcal{M}_n(K)$.

2.2.5 Agrégation Epreuve MG-2024 : description et premières impressions

Quelques réflexions à chaud (le lendemain en fait) sur cette épreuve de mathématiques générales 2024. Il est quand même mieux d'avoir le sujet sous la main avant de suivre la vidéo, sous peine de subir un triste monologue de 55 minutes : -)

Merci à Sydney Segovia pour son envoi d'une preuve de la 11a) plus simple que celle que j'avais rédigée ! Je la présenterai bientôt sur la chaîne.

2.2.6 Epreuve MG-2023 Partie II

La partie II nous invitait à étudier l'action du groupe orthogonal par conjugaison sur l'ensemble des matrices nilpotentes de taille n et d'indice 2. On exhibait une forme normale pour chaque orbite de l'action.

2.2.7 MG-2023 La partie I

La partie I du problème de l'épreuve MG-2023 parlait de la décomposition en valeurs singulières. Une preuves élégante posée sur la géométrie des espaces vectoriels réels, la notion d'application linéaire adjointe, ce qui demandait aux candidats de réviser un peu leur copie par rapport au programme qui assure des propriétés sur les « endomorphismes adjoints ». Au final, le théorème spectral finit tout de même par pointer son bout de nez.

2.2.8 MG-2023 Les exercices

Voici une proposition de solution sur les trois exercices. Attention, certaines images peuvent heurter la sensibilité de certains agrégatifs

2.2.9 Epreuve de mathématiques générales 2023

Un tour d'horizon de l'épreuve MG-2023 qui s'est déroulée hier. Au menu, un peu de groupes, d'arithmétique, mais surtout de l'algèbre linéaire, du théorème spectral et pour les plus aventureux, des matrices nilpotentes.

2.2.10 MG-2022-question 2-6a (le retour !)

Un retour d'Arthur Meyer qui nous a fait une proposition convaincante sur la question $6a$, et qui utilise la question précédente dans l'esprit du problème, réglant à la fois un problème mathématique et la paix dans le monde !

2.2.11 MG-2022 - Problème - Parties - V et VI

Correction des parties V et VI du problème de mathématiques générales 2022

2.2.12 MG-2022 - Problème - Parties - III et IV

Correction des parties III et IV du problème de mathématiques générales 2022

2.2.13 MG-2022 - Problème - Parties - I et II

Correction des parties I et II du problème de mathématiques générales 2022

2.2.14 Epreuve MG-2022 - Exercice - 3 et 4

Une fois passés les embouteillages des deux premiers exercices, la circulation devient plus fluide : avec un minimum d'habitude des corps finis et des p-groupes, on circulait sans encombre dans les exercices 3 et 4.

2.2.15 Epreuve MG-2022 - Exercice - 2

L' exercice 2 était sympathique jusqu'à la question 6 qui a dû renvoyer pas mal de candidats dans les cordes ! Mais abandonner est parfois plus dur que persévérer, et il faut parfois savoir sauter des par dessus les questions, quitte à transformer l'épreuve en un 110 mètres haie.

2.2.16 Epreuve MG-2022 - Exercice - 1

Pas si simple cet exercice 1... Mais enfin, fallait regarder ma chaîne où l'on a dévoilé tous les arcanes des équations matricielles : -)

2.2.17 Epreuve MG-2022 - Discussion

Cette année, de la théorie des représentations dans le problème, mais était-il possible en 6 heures d'y accéder pour la plupart des candidats, avec des exercices à tiroirs et parmi eux, quelques questions où l'on pouvait facilement s'embourber. Vous allez me dire, il n'y a qu'à les sauter, et hop ! Pas si simple quand le jury annonce une politique anti-grapillage...

2.2.18 Prélude au problème MG-2022 (théorie des représentations)

Nous avons corrigé les 4 exercices de l'épreuve maths géné de l'agrégation externe 2022. Nous allons maintenant tenter de corriger le problème qui se trouve être le premier (et certainement pas le dernier) problème sur la théorie des représentations à l'agrégation externe. Mais, dans cette théorie, il est surtout important de se familiariser avec les objets et les méthodes. Ce que nous allons faire dans un premier temps...

2.2.19 Epreuve Agrégation Externe - MG-2021 - Partie II ($Q1$ à 4)

On attaque la partie II du problème, questions de 1 à 4. Le but est de montrer que si A est principal (et infini), on peut toujours trouver une A-base échelonnée (appelée base régulière) de Ent (A) (les polynomes de Frac $(A)[X]$ à valeurs dans A pour tout a de A). C'est une généralisation des polynômes de Hilbert.

2.2.20 Epreuve Agrégation Externe - MG-2021 - Fin de la partie I

On achève ici la partie I, où l'on utilise les propriétés des polynômes de Hilbert pour caractériser les polynômes de $\mathbb{Q}[X]$ de degré n qui prennent des valeurs entières sur $\mathbb{Z}$.

2.2.21 Epreuve Agrégation Externe - MG-2021 - Partie I-Q4-5-6-7

On reste concentré !

2.2.22 Epreuve Agrégation Externe - MG-2021 - Partie I-Q1-2-3

C'est fou ce que peut faire un carré de chocolat dans un cerveau fatigué par quatre exercices d'agreg !

2.2.23 Epreuve Agrégation Externe - MG-2021 - Exercice 4

L'exercice 4 (le dernier avant d'attaquer le problème vise à montrer que si p est premier toute fonction de $\mathbb{Z}/p\mathbb{Z}$ dans lui-même se réalise à l'aide d'un polynôme de $\mathbb{Z}/p\mathbb{Z}[X]$. Mais c'est tout de suite faux si p n'est pas premier, à commencer par $p = 4$.

2.2.24 Epreuve Agrégation Externe - MG-2021 - Exercice 3

Un petit exercice qui, tout en restant dans la thématique du problème, nous permet de faire un petit tour du côté des matrices, utiliser le morphisme d'évaluation et même Cayley-Hamilton (soyons fous).

2.2.25 Epreuve Agrégation Externe - MG-2021 - Exercice 2

L' exercice 2 portait sur une preuve

polynomiale du déterminant de Vandermonde. Amusant, c'était justement dans les Carnets de Voyage en Algébrie (remarque 1. 3. 4). Ceci nous permet de comprendre pourquoi, si $\mathbb{K}$ est une extension du corps k, un polynôme de $\mathbb{K}[X]$ qui envoient k sur k, sont automatiquement dans $\mathbb{K}[X]$.

2.2.26 Epreuve Agrégation Externe - MG-2021 - Exercice 1

On commence une petite correction, à la volée, du problème de math géné 2021 à l'agrégation externe de mathématiques. Au menu, une intéressante incursion dans la problématique des polynômes respectant un anneau fixé. Les polynômes de Hilbert constituent un petit apéritif pour nous montrer qu'un polynôme de $Q[X]$ respectant $\mathbb{Z}$, n'est pas forcément dans $\mathbb{Z}[X]$.

2.2.27 Résumé sur l'épreuve MG-2021-4

Le mot de la fin sur l'épreuve MG-2021 de l'agrégation externe. Il était temps de conclure.

2.2.28 Résumé sur l'épreuve MG-2021-3

Pas description, tout est dans la vidéo.

2.2.29 Résumé sur l'épreuve MG-2021-2

Pas description, tout est dans la vidéo.

2.2.30 Résumé sur l'épreuve MG-2021-1

Pas description, tout est dans la vidéo.

2.2.31 MG-2021. Exemples de polynômes envoyant une suite d'entiers sur $\mathbb{Z}$

La plus jolie partie (à mon goût) du III de l'épreuve Maths Géné de 2021. On envoie la suite des carrés, une suite géométrique sur les entiers et on se retrouve capables de trouver tous les polynômes qui envoient cette suite sur des entiers. Ce sont des suites dans lesquelles on a finalement trouvé un p-ordre ne dépendant pas de p. Saurez-vous trouver d'autres suites sur lesquelles un tel ordre est possible ?

2.2.32 L'algorithme LLL (Lenstra - Lenstra - Lovasz) : MG 2020 Agrégation externe 11

On expose très brièvement un algorithme qui permet de transformer une base d'un réseau de $\mathbb{R}^n$, en une base du même réseau permettant d'obtenir une base d'orthogonalisation à la Gram-Schmidt dont les vecteurs ne décroissent pas trop rapidement en norme. Cet algorithme a été motivé dans la vidéo 9 lorsque l'on voulait déterminer, en un temps polynomial en n, un vecteur de norme assez petite dans un réseau.

2.2.33 Inégalité de Minkowski sur les réseaux : MG 2020 Agrégation externe 10

Une preuve simple de l'inégalité de Minkowski qui majore le plus petit vecteur d'un réseau.

2.2.34 Le problème du plus petit vecteur d'un réseau : MG 2020 Agrégation externe 9

On a vu comment passer d'un problème de factorisation dans $\mathbb{Z}[X]$ à un problème de recherche d'un vecteur de norme minimale dans un réseau de $\mathbb{R}^n$. Dans cette vidéo on donne une borne min et une borne max pour ce plus petit vecteur, bornes qui s'expriment en fonction de la norme des vecteurs de la base orthonormalisée (par Gram-Schmidt) d'une base fixée du réseau. La borne min va utiliser encore une fois la décomposition QR et la borne max l'inégalité de Minkowski dans les réseaux.

2.2.35 Réseaux en cryptographie : MG 2020 Agrégation externe 8

On attaque l'articulation du problème d'agrégation MG 2020. Il s'agissait de comprendre un algorithme permettant de factoriser les polynômes dans $\mathbb{Z}[X]$. On commence par regarder la factorisation du polynôme donné modulo p assez grand par la méthode de Cantor-Zassenhaus (vue précédemment), puis les inégalités d'Hadamard sur le résultant permettent de remonter des informations de $\mathbb{Z}/p\mathbb{Z}$ à $\mathbb{Z}$! On est amené à déterminer un vecteur de norme minimale dans un réseau.

2.2.36 Le résultant : MG 2020 Agrégation externe 7

On présente ici succinctement le résultant. Il s'agit d'un déterminant qui permet de voir si deux polynômes sont ou non premiers entre eux. Lorsque les deux polynômes sont à coefficients entiers, on peut les réduire modulo p premier et voir, grâce à la réduction du résultant, si les deux polynômes réduits sont ou non premiers entre eux. Si p est assez grand par rapport aux coefficients des deux polynômes, l'inégalité d'Hadamard va montrer que les deux polynômes sont premiers entre eux dans $\mathbb{Z}$ si et seulement s'il sont premiers entre eux sur $\mathbb{Z}/p\mathbb{Z}$. C'est d'autant plus fort que la décomposition modulo p est plus simple à vérifier que dans $\mathbb{Z}$.

2.2.37 Cantor-Zassenhaus : MG 2020 Agrégation externe 6

On procède maintenant à la seconde étape de la factorisation d'un polynôme sur $\mathbb{Z}/p\mathbb{Z}$. La première étape nous ramène au cas où f se décompose en facteurs irréductibles de même degré d. On utilise une méthode probabiliste audacieuse due à Cantor et Zassenhaus : on choisit un polynôme g de degré strictement inférieur à celui de f. Si pgcd (f, g) est non trivial, on casse le polynôme en deux et on continue sur ses morceaux. Si pgcd $(f, g) = 1$, on remplace g par $g^k - 1$ avec $k = (p^d - 1)/2$ et on voit que l'on toutes les chances d'obtenir pgcd (f, g) est non trivial avec ce nouveau polynôme g.

2.2.38 Cantor-Zassenhaus : MG 2020 Agrégation externe 5

Une factorisation d'un polynôme sur $\mathbb{Z}/p\mathbb{Z}$ peut être une bonne étape pour la factorisation sur $\mathbb{Z}$. On commence pour cela par factoriser le polynôme de $\mathbb{Z}/p\mathbb{Z}[X]$ en polynômes u_d, non nécessairement irréductibles, tels que leurs facteurs irréductibles soient de degré d. On montre dans cette vidéo comment effectuer cette première étape. Cette « stratification » par les polynômes u_d utilise le fait que $\mathbb{F}_p$ est un corps parfait, ou, plus simplement, que les polynômes $X^{p^d} - X$ n'ont pas de multiplicité quand on les décompose en facteurs de degré 1. Ensuite, on utilise un simple algorithme d'Euclide. On verra la seconde étape dans la prochaine vidéo.

2.2.39 Gram-Schmidt, QR et inégalité d'Hadamard : MG 2020 Agrégation externe 4

Voici un lien classique (déjà discuté dans la vidéo 2 du « théorème du confinement ») entre la méthode d'orthogonalisation de Gram-Schmidt, la décomposition QR, et l'inégalité d'Hadamard.

2.2.40 Borne de Cauchy : MG 2020 Agrégation externe 3

On montre l'inégalité dite de la borne de Cauchy qui donne un bon majorant pour les module des racines d'un polynôme complexe P. On va en donner un corollaire qui donne une borne aux modules des coefficients des polynôme unitaires qui divisent P.

2.2.41 Suites arithmético-géométriques : MG 2020 Agrégation externe 2

On présente les suites arithmético-géométriques dans $\mathbb{C}^n$. Ce sont des suites de vecteurs de la forme $X_{n+1} = AX_n + B$, où A est une matrice carrée et B un vecteur. Si 1 n'est pas dans le spectre de A, alors, c'est moralement une suite géométrique (à changement de variable près) et si A est la matrice identité, c'est une suite arithmétique. Dans les cas qui vont nous intéresser, c'est le lemme des noyaux qui fera le tri.

2.2.42 Agrégation externe : épreuve MG 2020- 1

En attendant les résultats (demain normalement)... On présente le problème de l'épreuve de mathématiques générales 2020 en mathématiques. On présente les différentes composantes du problème, ses qualités et ses défauts, autant dans son intérêt mathématique que dans ses capacités évaluatrices. Dans les prochaines vidéos (de 2 à 11), on rentrera dans les détails, sans toutefois se substituer à un corrigé.

2.2.43 MG-2018 - Les exercices préliminaires

Une correction de la partie « exercices préliminaires » du problème de mathématiques générales de 2018.

2.2.44 Conseils autour de l'épreuve MG-2018 Agrégation Externe

Un petit debriefing autour de cette épreuve qui mêlait algèbre linéaire et (un peu d') analyse complexe. Au programme : comment sortir d'une épreuve écrite en optimisant la note ! Il y avait au menu de cette année là : Décomposition de Dunford, polynômes d'interpolation, exponentielle et logarithmes, et un peu de représentations, pour la forme -de façon très superficielle- et aussi pour le fond- de façon trop profonde pour que ce soit utile en tant que candidat. Au passage, après un coup de téléphone du livreur, je fais de la pub pour le livre de la prépa Lyon : Carnet de Voyage en Analystan publié aux éditions de l'IREM !

2.2.45 Le problème de Dirichlet (Epreuve AP-2019)

Voici une preuve du théorème de prolongement de Dirichlet qui assure qu'une fonction continue sur le disque unité peut être prolongée de façon unique par une fonction harmonique sur le disque unité. La preuve suit la partie III de l'épreuve d'analyse AP-2019.

2.2.46 Agrégation externe Epreuve MG-2025 : description et premières impressions

Quelques réflexions à chaud sur l'épreuve de mathématiques générales 2024. Il est quand même mieux d'avoir le sujet sous la main avant de suivre la vidéo, sous peine de subir une heure de litanie.

2.2.47 MG-2025-Exercice préliminaire

Une correction orale de l'exercice préliminaire de l'épreuve MG-2025.

2.2.48 MG-2025-Partie I

La partie I de l'épreuve de math générale 2025 commence avec quelques "questions de cours" en théorie des corps : on regarde les propriétés de éléments algébriques ou transcendants sur un corps donné, et on dévoile les mystères de son polynôme minimal qui, bien qu'irréductible sur le corps de base, peut se révéler à racine multiples si le corps montre quelques imperfections... On étudie ensuite en deux temps la réduction de l'endomorphisme de multiplication par un élément x d'une extension finie L d'un corps K. D'abord, si L=K(x), où l'on retrouve avec bonheur la matrice compagnon, puis dans le cas général où l'on va dézoomer à l'aide d'une base qui porte bien son nom !

2.2.49 MG-2025-Partie II

Sans vraiment rentrer dans le dur, on rentrait dans le vif du sujet : les dérivations sur un corps et leur prolongement sur une extension du corps. On commence par quelques calculs lénifiants (mais nécessaires) pour continuer avec le cas de la caractéristique nulle, dans lequel on montre à l'aide d'une formule élégante, que les dérivations se prolongent de façon unique. Le cas des corps finis donnent des dérivations triviales mais on n'a pas unicité du prolongement en caractéristique p (un contre-exemple nous est donné sur un corps non parfait).

2.2.50 MG-2025-Partie III ou presque

On y aura mis le temps, mais nous voici arrivés au but ultime de l'épreuve. Dans un premier temps, on définit la notion de logarithme et exponentielle dans un extension de corps différentielle. On trouve des conditions simples pour qu'une exponentielle soit algébrique sur un corps. Après en avoir donné une application au cas des extensions sur le corps C(X) muni de sa dérivée usuelle, on donne ensuite un analogue logarithmique de la condition.

Puis, arrive le problème de condition d'existence d'une primitive dans une extension (finie/logarithmique/exponentielle)... Dur problème qui, dans le cas algébrique se démêle par la trace, mais dans le cas transcendant donne du fil à retordre ! On n'ira malheureusement pas jusqu'au bout (problème d'inspiration dans la question 44...)

2.3 Agreg-Docteur

2.3.1 Trace et nilpotence-Agreg-Docteur-2024

Une variante originale du critère de nilpotence par trace dans un exercice donné au concours de l'agrégation spéciale docteur 2024. On pourra retrouver avec bonheur d'autres preuves similaires dans Carnet de Voyage en Algébrie.

2.3.2 Agreg Docteur 2025- Problème d'Algèbre

Un joli problème (d'ailleurs assez proche en considérations avec des choses que l'on trouvera avec bonheur dans Carnet de Voyage en Algébrie !) qui parle de sous-espaces de matrices toutes singulières. Ce problème coche pour moi toutes les valeurs d'une épreuve d'agrégation : une thématique au coeur du programme, une mobilisation autour d'un résultat pas très connu (mais un peu quand même), une progression ente avec des choses plus borderline. Bref la continuité dans le changement, selon l'adage de Tonton François !

2.3.3 Agreg-Docteur-2025-Pb Algèbre Partie I-II

Quoi de neuf Doc ? Et bien le corrigé des deux premières parties du joli problème d'algèbre de l'épreuve 2025. On montre qu'un sous espace de matrices de taille n sur un corps K, n'intersectant pas $\mathrm{GL}_n(K)$ est de codimension supérieure à n. Dans un premier temps on montre avec élégance que la codimension est supérieure à 2. Des résultats (et parfois des preuves) très proches de ceux que l'on peut trouver dans Carnet de Voyage en Algébrie !

2.3.4 Agreg-Docteur-2025-Pb Algèbre Partie III-IV

Nous caractérisons ici les sous-espaces de matrices extrémaux (dans le sens, de dimension $n(n-1)$) n'intersectant pas GL_n. On utilise pour cela, toute la théorie dont on dispose sur le rang (formule du rang, théorème du rang, caractérisation par les mineurs, action de Steinitz...) et des résultats standards sur les formes quadratiques non dégénérées.

2.3.5 Endomorphismes qui stabilisent GLn(K)-MD-2025-Partie V

C'est un résultat folklorique de classe prépa et d'agrégation qu'un endomorphisme de $M_n(K)$ qui stabilise les matrices inversibles respecte le rang. Ici, nous allons voir une preuve originale qui utilise la classification des sous-espaces de $M_n(K)$ de dimension n^2-n qui n'intersectent pas GL_n. Nous allons même plus loin en classifiant ces endomorphismes modulo action de Steinitz : on n'a que deux orbites, l'orbite de l'identité et celle de la transposition !

2.4 Agrégation interne

2.4.1 Epreuve 1 - Agrégation interne 2024

Quelques commentaires à chaud sur la première épreuve d'agrégation interne de 2024.

2.4.2 Epreuve 1 - Agrégation interne 2024 - Exercice 1 (le vrai-faux)

Le vrai-faux de l'épreuve 1 (exercice 1)

2.4.3 Epreuve 1 - Agrégation interne - 2024 - Exercice 2

L'exercice 2 de EP1-2024

2.4.4 Epreuve 1 - Agrégation interne - 2024 - Exercice 3

L'exercice 3 de EP1-2024

2.4.5 Epreuve 1 - Agrégation interne - 2024 - Questions 10 et 11

Les questions 10 et 11 de EP1-2024

2.4.6 Epreuve 1 - Agrégation interne - 2024 - Questions 12 à 16

Les questions 12 à 16 de EP1-2024

2.4.7 Epreuve 1 - Agrégation interne - 2024 - Questions 17 à 21 (Partie IV)

Les questions 17 à 21 (Partie IV)

2.4.8 Epreuve 1 - Agrégation interne - 2024 - Questions 22 à 25 (Partie V)

Les questions 22 à 25 (Partie V)

2.4.9 Epreuve 1 - Agrégation interne - 2024– (Partie VI)

Et on finit avec la partie VI

2.4.10 La théorie des représentations post EP1-2024

Après avoir fini la correction de l'épreuve EP1-2024 qui abordait la théorie des caractères, on peut, pour ceux qui en ont pris plaisir et ceux que cela intéresse, en profiter pour parler des développements de la théorie.

2.4.11 EP1 - Agreg interne 2023 ou le théorème de Skolem-Mahler

Le théorème de Skolem-Mahler parle des zéros d'une suite récurrente linéaire entière. Il peut se faire avec les entiers p-adiques, mais l'épreuve de 2023 admettait un théorème un peu lourd de zéros isolés dans le cas p-adique, ce qui est, on l'admettra, bien dommage. On reprend ici la preuve du problème, mais on donne une preuve plus complète qui n'utilise que le corps des rationnels.

2.4.12 Epreuve EP1-2023 - Agrégation Interne - Problème I-C

On continue la correction de l'épreuve EP1-2023 avec la partie I-C du problème, où l'on s'intéresse à un caractérisation des puissances de 2 par les nombres binomiaux.

2.4.13 Epreuve EP1-2023 - Agrégation Interne - Problème I-B

On continue la correction de l'épreuve EP1-2023 avec la partie I-B du problème, où l'on prouve par une méthode élégante, la formule de Legendre.

2.4.14 Epreuve EP1-2023 - Agrégation Interne - Problème I-A

On continue la correction de l'épreuve (tristounette, faut reconnaître) EP1-2023. On trouvera ici la partie $I - A$ du problème.

2.4.15 Epreuve EP1-2023 - Agrégation Interne-Vrai-Faux et Exercices

On commence une correction de l'épreuve EP1-2023. Ici, on trouvera le vrai-faux, et les deux premiers exercices. C'est-à-dire largement de quoi être admissible !

$*$ Errata ! J'ai trop vite lu l'énoncé, dans la question $1e$) du Vrai-Faux, $\mathbb{L}$ et $\mathbb{K}$ sont des corps et non des anneaux. Si c'est un morphisme d'anneaux unitaires (ce que je suppose), il est non nul, donc le noyau, qui est un idéal de $\mathbb{K}$ est forcément trivial. Du coup, le morphisme mu est injectif. Et l'assertion est VRAIE ! Toutes mes excuses pour le désarroi que cela a pu créer !

2.4.16 Epreuve 1-2022 de l'agrégation interne - 9 (Les réseaux à l'agreg !)

On a déjà fait une série de videos sur les réseaux à l'agrégation, mais quoi de mieux que de le faire sur l'exemple ! ici, il s'agit de la partie VIII de l'épreuve 1 de l'agrégation interne de 2022.

2.4.17 Epreuve 1-2022 de l'agrégation interne - 8 (Survol des parties restantes)

Après avoir corrigé en détail jusqu'à la partie IV, on finit par un grand balayage, façon salon de coiffure, des parties de l'épreuve 1 de l'agrégation interne 2022. Le bonheur est-il au bout de l'ascension ? On verra tout de même que la fin proposait des idées intéressantes sur des théorèmes de descente sur $\mathbb{Z}$ par la théorie des réseaux.

2.4.18 Epreuve 1-2022 de l'agrégation interne - 7 (la partie IV)

On se propose ici de donner des éléments de correction de l'épreuve 1 de l'agrégation interne 2022, et ce, jusqu'à la partie IV, car il serait étonnant que *quelqu'un* soit allé plus loin. L'objectif ici est plutôt de voir un peu ce qui était faisable plutôt que de regarder ce joli problème dans son ensemble. Voici maintenant la partie IV, qui demandait une certaine expérience sur les extensions de corps. On arrêtera les corrections détaillées sur cette partie.

2.4.19 Epreuve 1-2022 de l'agrégation interne - 6 (la partie III)

On se propose ici de donner des éléments de correction de l'épreuve 1 de l'agrégation interne 2022, et ce, jusqu'à la partie IV, car il serait étonnant que *quelqu'un* soit allé plus loin. L'objectif ici est plutôt de voir un peu ce qui était faisable plutôt que de regarder ce joli problème dans son ensemble. Voici maintenant la partie III, qui concerne l'étude d'une extension de corps (mais sans vraiment le dire, car ce n'est pas au programme, et en plus, on n'a pas besoin de l'outillage habituel de la théorie)

2.4.20 Epreuve 1-2022 de l'agrégation interne - 5 (la partie II)

On se propose ici de donner des éléments de correction de l'épreuve 1 de l'agrégation interne 2022, et ce, jusqu'à la partie IV, car il serait étonnant que *quelqu'un* soit allé plus loin. L'objectif ici est plutôt de voir un peu ce qui était faisable plutôt que de regarder ce joli problème dans son ensemble. Voici maintenant la partie II, avec au programme des fonctions symétriques élémentaires, des fonctions invariantes par similitude, et surtout, de l'arithmétique modulaire. C'est malgré tout une partie assez simple (quand on s'y connaît un minimum).

2.4.21 Epreuve 1-2022 de l'agrégation interne - 4 (la partie I)

On se propose ici de donner des éléments de correction de l'épreuve 1 de l'agrégation interne 2022, et ce, jusqu'à la partie IV, car il serait étonnant que quelqu'un soit allé plus loin. L'objectif ici est plutôt de voir un peu ce qui était faisable plutôt que de regarder ce joli problème dans son ensemble. Voici maintenant la partie I où il était question de racine n-ième d'une matrice symétrique positive réelle de taille p.

2.4.22 Epreuve 1-2022 de l'agrégation interne - 3 (l'exercice préliminaire)

On se propose ici de donner des éléments de correction de l'épreuve 1 de l'agrégation interne 2022, et ce, jusqu'à la partie IV, car il serait étonnant que *quelqu'un* soit allé plus loin. L'objectif ici est plutôt de voir un peu ce qui était faisable plutôt que de regarder ce joli problème dans son ensemble. Voici maintenant l'exercice préliminaire (on devrait dire l'enquête préliminaire ?) où il était question de prouver, si besoin est, le théorème de Cayley-Hamilton.

2.4.23 Epreuve 1-2022 de l'agrégation interne - 2 (le vrai-faux)

On se propose ici de donner des éléments de correction de l'épreuve 1 de l'agrégation interne 2022, et ce, jusqu'à la partie IV, car il serait étonnant que *quelqu'un* soit allé plus loin. L'objectif ici est plutôt de voir un peu ce qui était faisable plutôt que de regarder ce joli problème dans son ensemble. On attaque le « vrai-faux », une nouveauté dans l'épreuve.

2.4.24 Epreuve 1-2022 de l'agrégation interne - 1

On se propose ici de donner des éléments de correction de l'épreuve 1 de l'agrégation interne 2022, et ce, jusqu'à la partie IV, car il serait étonnant que *quelqu'un* soit allé plus loin. L'objectif ici est plutôt de voir un peu ce qui était faisable plutôt que de regarder ce joli problème dans son ensemble. Dans cette première partie, je vais donner de cette épreuve ma vision en tant que préparateur.

2.4.25 Epreuve 1 de l'agrégation interne 2021-6 : les corollaires du théorème de Burnside

On finit ce volet sur cette épreuve EP1-2021 de l'agrégation interne. On parlera en diagonale des corollaires du théorèmes de Burnside : 1) le groupe unitaire engendre comme espace l'algèbre $\mathcal{M}_n(\mathbb{C})$, 2) un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$ constitué d'éléments unipotent est co-trigonalisable, 3) le sous-espace des matrices magiques est engendré par les matrices de permutations. Tout se résume finalement en une alternative « semi-simplicité » ou « résolubilité » que l'on retrouve partout dans le monde de l'algèbre.

2.4.26 Epreuve 1 de l'agrégation interne $2021-5$: Quelques exemples sur Q

On achève la partie 3 avec la question 13. On bascule ici dans l'arithmétique et on en profite pour réviser nos classiques.

2.4.27 Epreuve 1 de l'agrégation interne $2021-4$: Quelques exemples

Nous voici arrivé à la partie 3 et il semble, au moins dans un premier temps, que l'orage est passé. Tels de petits écureuils, nous allons en profiter pour grappiller quelques points avant que cela ne se couvre.

2.4.28 Epreuve 1 de l'agrégation interne $2021-3$: théorème de densité de Jacobson (ou Burnside)

On finit en beauté la partie 2 avec la preuve du théorème de Burnside grâce à un résultat de semi-simplicité.

2.4.29 Epreuve 1 de l'agrégation interne $2021-2$: stabilité et semi-simplicité

On attaque le moment le plus intense de ce début de problème (qui en sera peut-être aussi la fin pour le candidat qui n'aura pas osé sauter ces questions). On transporte des problèmes d'irréductibilité dans End (E) à des problèmes de semi-simplicité dans End (E^n). C'est dans les deux dernières questions de la partie 2 que la beauté du raisonnement se révèlera au grand jour. Mais ce sera pour la vidéo prochaine...

2.4.30 Epreuve 1 de l'agrégation interne 2021-Préliminaires et palabres

Voici une petite présentation du problème proposé pour la première épreuve de l'agrégation interne 2021. Nous ne parlerons ici que des préliminaires sur la réduction, avant de présenter ce qui sera prouvé dans les prochaines vidéos, c'est-à-dire le théorème de Burnside à l'aide d'un théorème de densité dû à Jacobson.

2.4.31 Epreuve EP1 Agrégation interne $2020 - 2$

On vient de voir qu'un drapeau (total) possède une base adaptée. On va l'appliquer au drapeau des noyaux emboîtés d'un endomorphisme, ce qui va nous fournir un drapeau stable par l'endomorphisme en question. On en profite pour prouver ce résultat souvent utile qui stipule que la suite des dimensions des noyaux emboîtés « s'essouffle ». On montre ensuite que le groupes des matrices triangulaires supérieures unitaire est distingué dans le groupe des matrices triangulaires supérieures inversibles. Toutefois, il n'est en général pas distingué dans le groupe linéaire.

2.4.32 Epreuve EP1 Agrégation interne $2020 - 1$

On va parler ici du problème d'agrégation interne $2020(EP1)$. Au programme, la définition d'un drapeau total (suite emboitée de sous-espaces E_i tels que $\dim E_i = i$), l'existence d'une base adaptée pour un drapeau total, et orthonormée adaptée dans le cadre d'une espace euclidien. Enfin, on montre donne de trigonalisabilité : un endomorphisme est trigonalisable si et seulement si l'on peut trouver un drapeau stable pour cet endomorphisme.

2.4.33 Polynômes d'Hermite - EP2 - Agrégation interne - 2019

La seconde épreuve à l'agrégation interne de 2019 parlait des polynômes d'Hermite en première partie. Nous allons suivre la trame de l'épreuve pas à pas, à la découverte de l'univers des polynômes orthogonaux. Au menu, Gram-Schmidt et intégration par partie.
La seconde épreuve à l'agrégation interne de 2019 parlait des polynômes d'Hermite en première partie. Nous allons suivre la trame de l'épreuve pas à pas, à la découverte de l'univers des polynômes orthogonaux. Au menu, petites formules classiques, mais surtout une jolie technique qui marche tout le temps pour montrer que les polynômes orthogonaux sont scindés simples sur $\mathbb{R}$.
On sort ici du cadre de l'épreuve EP2- Agrégation interne de 2019, pour parler pour parler justement des classiques du genre auxquels nous avions échappés cette année-là. Tout d'abord l'entrelacement des racines entre deux polynômes orthogonaux successifs, et ensuite l'application historique des polynômes orthogonaux aux calculs d'intégrales par la méthode de quadrature de Gauss.

2.4.34 Agrégation interne Epreuve 1 2018-4

Correction du problème de 2018 en Algèbre que lon peut trouver sur `https://interne.agreg.org/data/uploads/epreuves/ep1/18-ep1.pdf`On attaque ici les parties suivantes où l'on montre que l'ensemble Omega, sur lequel il était bien agréable de travailler, est dense dans $\mathcal{M}_n(\mathbb{C})$. Ce qui va répandre la propriété (2) dans tout $\mathcal{M}_n(\mathbb{C})$. Au programme : résultant, discriminant d'un polynôme, et densité d'un ouvert algébrique (on montre en fait que si P est un polynôme non nul à n variables, l'ensemble des x de $\mathbb{R}^n$ tels que $P(x)$ est non nul, est dense dans $\mathbb{R}^n$).

2.4.35 Agrégation interne Epreuve 1 2018-3

Correction du problème de 2018 en Algèbre que l'on peut trouver sur `https://interne.agreg.org/data/uploads/epreuves/ep1/18-ep1.pdf`
On attaque la partie II du problème. Au programme : le polynôme caractéristique de AB est égal à celui de BA (par densité de GL_n sur les complexes), et comme conséquence, le fait que le polynôme caractéristique de C^*C est à coefficients dans $\mathbb{R}$. Pour finir, on montre que det $(I_n + C^*C)$ est positif sur un ensemble Omega de matrices $\mathbb{C}$.

2.4.36 Agrégation interne Epreuve 1 2018-2

Correction du problème de 2018 en Algèbre que lon peut trouver sur `https://interne.agreg.org/data/uploads/epreuves/ep1/18-ep1.pdf`
Dans cette vidéo, on corrige la densité de GL_n et la question 5 de la partie I. Ce qui achèvera la partie I, et nous mettra en bonne voie vers la partie II.

2.4.37 Agrégation interne Epreuve 1 2018-1

Correction du problème de 2018 en Algèbre que l'on peut trouver sur `https://interne.agreg.org/data/uploads/epreuves/ep1/18-ep1.pdf`
Dans cette vidéo, on corrige (oralement) la partie I (sauf la densité de GL_n et la question 5).

2.4.38 Exercices sur les homographies - EP1-2017

Un petit exercice de transformation homographique dans le style de la partie I de l'épreuve EP1 de l'agrégation interne 2017. On montre que la transformation de Cayley envoie la droite réelle sur le cercle unité. On montre ensuite que cette transformation envoie le demi-plan de Poincaré sur le disque ouvert unité, par deux méthodes, une calculatoire, et l'autre topologique.

2.4.39 2014-EP1 - Agrégation interne - parties-I-II

Pas description, tout est dans la vidéo.

2.4.40 Sujet EP1 - Agrégation interne - 2008 - Partie II

Voici maintenant la correction de partie II, on l'on verra que sur le corps des complexes, une sous-algèbre de End (E) n'ayant pour sous-espace stable que les sous-espaces triviaux est égale à End (E). On verra à la fin un contre - exemple sur $\mathbb{R}$, avec une sous-algèbre irréductible bien connue depuis la terminale (!).

2.4.41 Sujet EP1 - Agrégation interne - 2008 - Partie I

Le sujet EP1 d'agrégation interne de 2008 est particulièrement confondant : il ne demande que très peu de connaissance (projection, matrices élémentaires, sommes directes, dualité) mais une bonne maîtrise du sujet. Voici déjà la correction d'une partie I très instructive qui nous mènera au théorème de Skolem-Noether.

2.4.42 EP2-2025-TOUT sur l'ellipsoïde de John !

2.4.43 EP2-2025 Agrégation interne-Presentation

Petite discussion informelle sur l'épreuve 2 (reportée) de l'agrégation interne 2025. Entre plaisir (du mathématicien) et déception (du préparateur), on abordera ici les contours du problème. L'ellipsoïde de John y était à l'honneur,dans une version inhabituelle (plutôt duale à celle que l'on trouve dans les livres de développements) et plus complète, avec une caractérisation via une propriété ébouriffante des points de contacts !

On décompose maintenant l'épreuve en ces huit parties qui s'enchaînent comme du Mozart !

2.5 Concours Classes prépa

2.5.1 Mines-Ponts-Math2-MP-2024 - Partie-I

Un problème fort intéressant, mais ardu, où il est question de graphes aléatoires. On attaque ici la partie I sur la réduction des matrices d'adjacence de graphes.

2.5.2 Mines-Ponts-Math2-MP-2024 - Partie-II

On attaque ici la partie II, beaucoup plus simple. On commence gentiment avec quelques premières notions de graphes aléatoires à ensemble de sommets fixé.

2.5.3 X-ENS MP-2024-Correction Q1-8

Voici un début de correction/discussion autour del'épreuve X ENS MP de cette année. Cette année, le problème parle de combinatoire et probabilité sur les groupes finis, un thème souvent discuté sur cette chaîne.

2.5.4 X-ENS MP-2024-Correction Q9-15

Voici la suite de la correction/discussion autour du sujet X-ENS 2024 MP. Nous attaquons la seconde moitié de la partie I, donc les questions de 9 à 15. On termine sur un épilogue où l'on fait le point sur cette première partie et où l'on proposera des solutions parfois plus longues (!), souvent plus courtes. Je me permettrai d'émettre quelques opinions personnelles... mais qui suis-je pour juger ?

2.6 Olympiades mathématiques

2.6.1 Equation diophantienne aux Olympiades

Une petite équation diophantienne astucieuse qui demande juste un niveau « terminale option maths » mais surtout beaucoup d'amour et de passion...

2.6.2 Equation diophantienne, estivale... et cyclotomique

Une petite équation diophantienne proposée par notre collègue Bodo Lass. Elle pourra nous apprendre à mieux comprendre les diviseurs premiers des polynômes cyclotomiques ainsi que leur utilisation.

PS : C'est la deuxième fois que je poste cette vidéo mais la première version comportait de grossières erreurs de montage ! ! ! Shame on me !

2.6.3 Un problème de décimales aux Olympiades

Un problème rentré dans les annales des olympiades, et proposé par notre ami Antoine avec sa solution arithmétique pleine d'élégance.

2.6.4 Dernières décimales de n^{10^d} (aux olympiades ou plus si affinités)

Un petit exercice d'olympiades en arithmétique. Au programme : congruence, indicatrice d'Euler, groupe des inversibles de l'anneau $(Z/nZ)^*$.

2.6.5 Triangles équilatéraux et nombre d'or

Un bel exercice, proposé par Jean-Jacques Juré, et donné aux Olympiades mathématiques sur une construction d'un triangle équilatéral à partir d'un autre, selon une égalités de surfaces. On en propose ici une preuve de type « Master » avec de la réduction de matrices, et une autre, plus élémentaire, qui peut, théoriquement, être faite en lycée. On pourra en tirer, une construction à la règle et au compas pour les nostalgiques et une formule matricielle par affixes qui a permis à Jean-Jacques d'intégrer la construction dans la rétine du héros de manga Itachi Uchiwa.

2.6.6 Triangles équilatéraux et nombre d'or-2

Après une remarque de Denis, je reprends cette vidéo sur la divine proportion dans un triangle équilatéral. Ceci nous permet de prendre plus de recul sur la méthode par réduction des matrices, et de fournir à ce problème une solution de niveau collège... Bref, des problèmes à grande largeur de spectre comme on aimerait en voir plus souvent.

3 Les oraux (175)

3.1 Leçons (71)

3.1.1 Leçon 133/101- Groupe opérant sur un ensemble- Applications

Une leçon aussi riche que passionnante à laquelle on va se confronter au mépris du danger ! Et le danger ici, c'est qu'il y a tellement de belles choses à raconter qu'on pourrait s'y perdre.

On commence ici avec un 6 minutes sur la leçon. Allez, 9 minutes...

Quelques questions de jury. Elles tournent autour de l'utilisation de la définition des actions de groupes, via les morphismes de groupes, la formule des classes, le principe de conjugaison-translation, la possibilité de ramener un problème à sa forme normale, l'utilisation de l'isomorphisme canonique associé au morphisme d'action, le dénombrement d'une orbite par le calcul de l'ordre du stabilisateur...

Quelques développements que l'on pourra trouver dans Carnet de Voyage en Algébrie et Nouvelles Histoires Hédonistes de Groupes et de Géométries.

3.1.2 Leçon $158-$ Groupe opérant sur un ensemble-1

Une leçon en 15 minutes par Magali, dans le cadre de l'oral de l'agrégation interne.

3.1.3 Leçon-158-Développement-Coloriage du tétraèdre

Voici un développement de Magali sur la leçon. Il s'agit du coloriage équivariant des faces d'un tétraèdre (Nouvelles Histoires Hédonistes de Groupes et de Géométries XII-B-7)

3.1.4 Leçon $105-$ Groupe de permutations d'un ensemble fini- Applications-6 minutes et plan

La leçon 105 (102 pour l'agrégation interne) parle d'un groupe, et pas n'importe lequel : le groupe des permutations d'un ensemble fini. On verra pourquoi ce groupe peut être vu comme la mère porteuse de tous les groupes finis, puis on en détaillera l'étude, selon la procédure à suivre pour tout bon groupe qui se respecte : générateurs, classes de conjugaisons, sous-groupes distingués, caractères, avant d'attaquer les nombreuses (et surtout diverses !) applications.

3.1.5 Leçon $105-$ Groupe de permutations d un ensemble fini et applications - les développements.

On présente une série de développements classiques et moins classiques autour de la leçon sur les groupes de permutations. On tentera pour chaque développement de décrire les grandes lignes de la preuve.

3.1.6 Leçon 105– Groupe de permutations d'un ensemble fini, applications - questions de jury et exercices

Quelques exercices simples ou parfois (clairement !) moins simples, tout en restant classiques, autour de la leçon sur le groupe symétrique. On utilise de façon essentielle : les systèmes de générateur de S_n, la formule de conjugaison, les centres, les groupes dérivés, l'ordre d'une permutation, la simplicité de A_n ainsi que les sous-groupes distingués de S_n, et bien sûr la signature, le hobbit de l'algèbre !

3.1.7 Leçon 106. Idéaux d'un anneau commutatif.

Une nouvelle leçon est apparue à l'agrégation interne, il s'agit de la leçon sur les idéaux. Cela demande un bagage important que la plupart des candidats ne possède pas, et pour commencer, la notion même de structure quotient doit être bien comprise. On va voir tour à tour, les idéaux, les générateurs d'idéaux, les opérations sur les idéaux, le passage au quotient et tout ce que cela implique. Dans un second chapitre on voit comment les idéaux principaux permettent de définir le pgcd, ppcm et une relation de Bezout. On déroule ensuite le rideau euclidien-principal-factoriel. Enfin le chapitre III est consacré aux applications des idéaux à l'étude des nombres premiers, en réduction, dans le systèmes de congruence, et même aux intersections de courbes planes.

3.1.8 Leçon 106/123-externe/interne : Groupe linéaire, sous-groupes et applications

Voici une vidéo qui présente (de façon relativement exhaustive, quoi que) de quoi remplir cette leçon sur le groupe linéaire. Cela pourra fournir des idées à certains, et pour d'autres, les aider à s'organiser sur un thème aussi riche !

3.1.9 Représentations linéaires d'un groupe fini 1 (leçon 107)

Il s'agit d'une vidéo de conseils sur la leçon 107 sur la théorie des représentation. Le principal conseil est de ne pas perdre pied avec l'aspect concret des choses. On fait ici la différence entre caractère et représentations, entre caractère irréductible et fonction centrale de norme 1. On donne des contre - exemples au théorème de Maschke et enfin, on décrit matriciellement toutes les définitions de base de la théorie ainsi que le théorème de Maschke.

3.1.10 Représentations linéaires d'un groupe fini 2 (leçon 107)

Un petit 6 minutes (qui dure en fait dix minutes) sur la théorie des représentations à l'oral de l'agreg externe.

3.1.11 Représentations linéaires d'un groupe fini 3 (leçon 107)

On propose ici deux petits exercices simples qui mettent le théorème de Maschke en relation avec la réduction. On propose ensuite quelques développements bienvenus dans la leçon.

3.1.12 Leçon 113 ou 152 : Déterminant et applications

Le déterminant est l'outil central de l'algèbre linéaire. On propose ici un 6 minutes (en fait, $6'40$ ") dans le cadre d'une leçon à l'agrégation externe (ou interne). Tout doit reposer sur le caractère n-linéaire alterné du déterminant qui lui permet de détecter les relations linéaires.

On passe ensuite à des petites questions de savoir-faire sur le déterminant dans le cadre de questions à un oral d'agrégation, puis, à quelques suggestions de développements que l'on peut trouver avec bonheur dans Nouvelles histoires hédonistes de groupes et de géométries et dans Carnet de Voyage en Algébrie.

3.1.13 Leçon 122-Anneaux principaux et applications - la présentation-1

La leçon sur les anneaux principaux constitue une belle occasion de réviser tout le programme d'algèbre (pas tout bien sûr, mais disons, le principal). On peut en effet se demander ce qui échappe à l'ubiquité de cette belle notion.

3.1.14 Leçon 122-Anneaux principaux et applications - 2

On regarde des petites propriétés générales (et des non propriétés également) des anneaux principaux. Passage à la localisation, (non) -passage à l'extension par une indéterminée. On exhibe des anneaux principaux, avec leurs inversibles, puis des anneaux non principaux, avec des (contre-) exemples d'idéaux non principaux.

3.1.15 Leçon 122-Anneaux principaux et applications - Evaluation-3

On peut évaluer des polynômes dans plusieurs contextes : l'évaluation de P dans $\mathbb{K}[X]$ en un élément a de $\mathbb{K}$, en plusieurs éléments a_i, l'évaluation en un élément algébrique sur $\mathbb{K}$, en une matrice (ou un endomorphisme), ou en un matrice localement en un éléments de l'espace. Dans tous les cas, des idéaux principaux apparaissent naturellement.

3.1.16 Leçon 122-Anneaux principaux et applications - Harmonisation-4

Voici venu l'instant d'émotion de la convergence des pôles. La théorie des groupes abéliens finis n'est en fait qu'une théorie de la réduction déguisée, et réciproquement. Cayley et Hamilton ne sont que des pseudos de Lagrange.

3.1.17 Leçon 122-Anneaux principaux et applications - Exercices-5

On commence maintenant dans cette vidéo et la suivante des petits exercices de jury (cad peu techniques, ni prise de tête, juste pour tester les réflexes et surtout la capacité de discuter avec un jury). Un exercice sur les polynômes qui s'annulent sur un corps fini, puis un problème d'irréductibilité d'un polynôme à plusieurs variables. C'est ici l'occasion de travailler sur un anneau principal bien choisi proche de l'anneau de départ (qui n'est pas principal).

3.1.18 Leçon 122-Anneaux principaux et applications - Exercices-6

Encore deux petits exercices assez rapides à poser et à résoudre dans le cadre des anneaux principaux.

3.1.19 Leçon 123 - Corps finis et applications

Voici de quoi remplir une belle leçon 123 sur le thème corps finis et applications. Tout d'abord quelques généralités où on parlera de ce que l'on peut dire a priori sur des corps finis, avant d'attaquer les théorèmes d'existence et d'unicité de ces corps finis. On parlera ensuite des corps finis en algèbre linéaire, dans la réduction, les formes quadratiques, puis, dans la théorie des extensions de corps et des polynômes irréductibles.

3.1.20 Leçon 125 - Extension de corps - exemples et applications - 1

On commence par quelques conseils, un 6 minutes, et quelques éléments à placer dans un plan pour cette leçon difficile.

3.1.21 Leçon 125 - Extension de corps - exemples et applications - 2

On passe (de façon progressive) aux questions de jury pour cette leçon 125.

3.1.22 Leçon 125 - Extension de corps - exemples et applications - 3

La chance ! Lipschitz, qui suit notre chaîne (continûment of course !), est passé l'an dernier (si je ne me trompe) sur la leçon, et il nous a envoyé la liste exhaustive des questions que le jury lui a posé. On fait en a sélectionné les plus intéressantes (il y avait aussi par exemple, comment montre-t-on Steinitz et fallait juste invoquer le nom sulfureux de Zorn).

3.1.23 Leçon 125 - Extension de corps - exemples et applications - 4

Cinq développements, sur la leçon 125 « extensions de corps, exemples et applications », un peu commentés, extraits de Cours d'Algèbre (Perrin), Carnet de Voyage en Algébrie (Caldero-Peronnier), et Nouvelles histoires hédonistes de groupes et de géométries (Caldero-Germoni)

3.1.24 Leçon 126 - Agrégation externe-équations en arithmétique-1

La leçon 126 est une modification de la leçon sur les équations diophantiennes. Mais avec le nouveau titre « équations en arithmétique » le spectre s'élargit considérablement. Il est temps de mettre de l'ordre dans nos idées !

3.1.25 Leçon 126 - Agrégation externe-équations en arithmétique-2

On tente un plan possible pour cette leçon. Parler tout d'abord, des équations linéaires, puis quadratiques, et enfin, le rôle des groupes dans les équations de l'arithmétique. Ce vole traîte rapidement (mais y -t-il beaucoup plus à dire ?) du cas linéaire.

3.1.26 Leçon 126 - Agrégation externe-équations en arithmétique-3

On se consacre aux équations quadratiques en arithmétique. En fait, pas toutes, parce qu'on garde le meilleur pour la fin, c'est-à-dire pour la partie III sur le thème groupes et géométries.

3.1.27 Leçon 126 - Agrégation externe-équations en arithmétique-5

On regarde ici les problèmes d'équations quadratiques qui peuvent se régler à l'aide de groupes (comme la loi de réciprocité quadratique, ou le cardinal d'une quadrique). Enfin, on parle de résultats en vrac, difficile à classer dans cette leçon (théorème de Chevalley-Warning, cardinal du cône nilpotent, équation de Fermat à l'ordre n)

3.1.28 Leçon 126 - Agrégation externe-questions de jury-6

Quelques équations typiques autour des techniques de base de la leçon (lemme de Gauss, lemme d'Euclide, Bezout, dénombrement de solutions à l'aide de séries génératrices, existence de solutions par cardinal d'une réunion, passage au quotient, cyclicité de $(\mathbb{Z}/p\mathbb{Z})^*$...)

3.1.29 Leçon 126 - Agrégation externe-questions de jury-7

Pour finir avec la leçon 126, une question de jury plus difficile (mais authentique !). Il s'agit d'une équation de Mordell, où il faut balayer le programme. Tout y passe, anneaux euclidiens, principaux, factoriels, unités de l'anneau, normes, éléments premiers entre eux... Mais ceci n'est que pretexte à discussion, personne ne s'attend à ce que vous puissiez résoudre une telle équation, où alors, ça cacherait quelque chose !

3.1.30 Leçon 127-Exemples de nombres remarquables-1

Une nouvelle leçon arrive cette année avec l'éternelle interrogation « peut-on recycler ce que l'on sait déjà avec les anciennes leçons, ou doit-on trouver de nouvelles idées et de nouvelles références ? » On va voir dans un premier temps que l'on peut placer des choses à peu de frais, mais il ne faut pas oublier que cette leçon est une leçon d'exemples et, à ce titre, demande au candidat une grande culture. Dans cette vidéo, nous parlerons de nombres décimaux, de décimales, de nombres algébriques et constructibles.

3.1.31 Leçon 127-Exemples de nombres remarquables-2

Une nouvelle leçon arrive cette année avec l'éternelle interrogation « peut-on recycler ce que l'on sait déjà avec les anciennes leçons, ou doit-on trouver de nouvelles idées et de nouvelles références ? » Dans cette vidéo, nous nous concentrerons sur la factorialité au service des équations diophantiennes, et, en particulier, à la décomposition en comme de carrés.

3.1.32 Leçon 127-Exemples de nombres remarquables-3

On attaque la partie « réelle » de la leçon, celle qui la distingue des autres : l'approximation diophantienne. Au programme : fractions continues, suites de Farey et nombres de Pisot.

3.1.33 Leçon 142 (ou 106) - PGCD et PPCM. Algorithmes et Applications-1

On attaque cette leçon par le début, c'est-à-dire que l'on part de l'acronyme PGCD, sa signification, et comment les propriétés de l'anneau (toujours intègre) dans lequel on se trouve (euclidien, principal, factoriel) fournissent l'existence, l'unicité, des propriétés bien naturelles, ainsi que des algorithmes (on verra les algorithmes plus en détails dans une vidéo prochaine) pour les calculer. On continue avec un exercice classique ainsi que, par pure curiosité, l'étude d'un anneau sans PGCD, et finalement, on verra que ça ne manque pas de piquant.

3.1.34 Leçon 142 (ou 106) - PGCD et PPCM. Algorithmes et Applications-2

On s'intéresse ici à l'identité de Bezout, si intimement liée à la notion de PGCD, valable uniquement dans un anneau principal. Dans ce premier volet sur cette identité, on va balayer les grands classiques (lien avec le lemme de Gauss, les inversibles des quotients). On donnera un contre - exemple dans un anneau factoriel (mais non principal) et deux petites questions de jury.

3.1.35 Leçon 142 (ou 106) - PGCD et PPCM. Algorithmes et Applications-3

On va parler de l'identité de Bezout dans ses applications. Tout d'abord, dans le lemme chinois, elle permet de trouver une expression explicite de l'antécédent, que ce soit dans le lemme chinois classique où les nombres sont premiers entre eux ou le lemme généralisé. Ensuite, elle permet de voir que le PGCD de polynômes de $\mathbb{K}[X]$ est invariant par extension de corps. Pour finir, en admettant un résultat sur le contenu, que nous verrons par la suite, on verra une application de l'identité de Bezout dans les problèmes d'intersection de courbes planes ! On rend alors à Bezout ce qui appartient à Bezout.

3.1.36 Le contenu de Gauss-Leçon $142(106)-4$

Pour une leçon 142 qui ne manque pas de contenu, optez pour Gauss ! On verra dans cette courte vidéo les preuves du théorème du contenu de Gauss (sur $A[X]$, A factoriel), une application aux irréductibles de $A[X]$, et deux exercices de jury.

3.1.37 La formule pgcd (a, b) ppcm (a , b) $= ab$ dans tous ses états-Leçon $142-5$

La formule pgcd (a, b) ppcm (a , b) $= ab$ n'est plus à présenter. Nous allons en voir tous les avatars à l'agrégation

3.1.38 Tout sur l'algorithme d'Euclide-Leçon 142-AE (ou $159-AI$) -6

Voici une présentation de l'algorithme d'Euclide que l'on peut trouver dans Carnet de Voyage en Algébrie. On sait en général trouver un PGCD à l'aide de l'algorithme d'Euclide, et on sait également « remonter à la main » les divisions successives de l'algorithme afin d'obtenir une relation de Bezout. Mais doit-on forcément remonter une par une ces divisions afin de trouver la fameuse identité ? La bonne nouvelle du jour, c'est que l'on a un ascenseur à disposition : une famille de polynômes, appelés polynômes continuants font le job. Non seulement ils fournissent la relation de Bezout de façon directe (si on connait ces polynômes une fois pour toutes), mais ils fournissent également une bonne borne pour complexité de l'algorithme. Cette borne est atteinte quand on part de deux nombres consécutifs de la suite de Fibonacci.

3.1.39 Invariants du groupe symétrique-142-Pgcd-7

Celui que je considère comme le plus joli développement sur le PGCD, que l'on peut trouver dans Carnet de Voyage en Algébrie. Il mélange PGCD, groupes cycliques, groupe symétrique, formes quadratiques réelles... et réduction si on peut placer une petite application.

3.1.40 Leçon 144-Racines d'un polynôme fonctions symétriques élémentaires

Voici une petite présentation des éléments à mettre (selon affinités) dans une leçon sur les racines d'un polynôme.

3.1.41 Racines d'un polynôme fonctions symétriques élémentaires 2 (leçon 144)

On continue sur la lecon 144 : racines d'un polynômes. On y propose les fondamentaux de la leçon, quelques petits exercices, et certains développements.

3.1.42 Leçon 144- Racines d'un polynôme - Questions de jury

Voici 8 questions de jury d'horizons diverses sur la leçon 144- sur les racines d'un polynôme et fonctions symétriques élémentaires

3.1.43 Leçon sur la dimension et le rang (148 ext/110 int) - Partie I.

La leçon sur dimension et rang est indémodable ! Mais comment mettre de l'ordre sur de telles notions fondamentales qui sont apparues dès le premier cours d'algèbre linéaire ? Voici déjà une première partie de plan sur la dimension qui je l'espère vous permettra de faire le point.

3.1.44 Leçon sur la dimension et le rang ($148ext/110$ int) - Partie II.

En ce début septembre, il est venu le moment de rentrer dans le rang ! Voici une seconde partie de plan où l'on va répertorier les hauts faits d'armes du rang : la formule du rang, l'invariance totale par changement de base, son comportement sur corps fini, sur les passages à la limite pour les espaces de matrices sur $\mathbb{R}$ ou $\mathbb{C}$, par extension de corps, et tout ce que cela entraîne dans l'univers de la réduction.

3.1.45 Leçon sur la dimension et le rang ($148ext/110$ int) - Partie III.

Voici quelques développements de tout niveau sur la leçon 148 pour l'externe et 110 pour l'interne. Avec des thèmes comme dimension et rang, le plus difficile est de faire son choix !

3.1.46 Leçon sur la dimension et le rang ($148ext/110$ int) - Partie IV.

Voici quelques questions de jury de niveau raisonnable sur la leçon 148*pour* l'externe et 110 pour l'interne.

3.1.47 Leçon $149-$ I-Généralités

Une leçon est tombée l'an dernier à l'agrégation externe « Valeurs propres - Vecteurs propres. Calculs exacts et Approchés des éléments propres. Applications. » On va donc commencer une petite série de vidéos sur le sujet. Pour commencer, voici quelques généralités qui permettent de bien démarrer sur cette leçon.

3.1.48 Leçon 149- II-Localisation des valeurs propres

Atour de cette leçon (un peu) nouvelle à l'agrégation externe « Valeurs propres - Vecteurs propres. Calculs exacts et approchés des éléments propres. Applications. » Voici donc une petite série de vidéos sur le sujet. Pour commencer, voici ce qui semble être le coeur de la leçon : localiser les valeurs propres, approximer les éléments propres. Au programme : rayon spectral, suites géométriques de matrices, méthode des puissances (et déflation si affinité), Perron-Frobenius, le tout, suivi de la méthode QR, et, pourquoi pas, le théorème d'entrelacement de Cauchy.

3.1.49 Leçon 149 - III - (Mais sans Elisabeth Borne)

Autour de la leçon tombée récemment à l'agrégation externe « Valeurs propres - Vecteurs propres. Calculs exacts et approchés des éléments propres. Applications. » Voici donc une petite série de vidéos sur le sujet. En voici donc quelques applications : Calcul approchés de racines de polynômes (via la matrice compagnon), suites récurrentes linéaires, allure de courbes solutions d'équations différentielles linéaires dans le plan réel, théorème de Kronecker, et bien sûr, une pléthore d'applications en théorie des représentations. Nous avons gardé pour une prochaine vidéo le lien entre valeurs propres et conditionnement d'une matrice.

3.1.50 Leçon 149– Valeurs propres, vecteurs propres. Calculs exacts ou approchés d'éléments propres.

Une leçon est tombée l'an dernier à l'agrégation externe « Valeurs propres - Vecteurs propres. Calculs exacts et Approchés des éléments propres. Applications. » On va donc commencer une petite série de vidéos sur le sujet. On commence par quelques commentaires au sujet du rapport sur cette leçon.

3.1.51 Actions de groupes sur les espaces de matrices (leçon 150)

Une quinzaine de minutes sur la présentation de la leçon Actions de groupes sur les espaces de matrices à l'oral d'agrégation externe.

3.1.52 Leçon- Formes linéaires, dualité. Exemples et Applications-I

Leçon 159 pour l'agrégation externe, 109 pour l'interne. Il s'agit d'une leçon délicate où les candidats peinent à trouver l'approche pertinente. Voici un 6 minutes et un session de questions de jury afin de préciser les choses.

3.1.53 Développements-Leçons formes linéaires, dualité.

Leçon 159 pour l'agrégation externe, 109 pour l'interne. Il s'agit d'une leçon délicate où les candidats peinent à trouver l'approche pertinente. Voici une liste de développements qui correspondent aux attendus.

3.1.54 Leçon 161-Distances et isométries d'un espace affine euclidien-1

La leçon 161 porte sur les isométries et distances en géométrie euclidienne (affine, mais on verra que c'est un pléonasme). On essaie de tailler un choix parmi les innombrables sujets que l'on pourrait exposer.

On amorce la première partie du plan, que l'on appelle en général... généralités. Une petite preuve du fait que toute isométrie est affine et une autre sur la réduction des endomorphismes orthogonaux. On parle aussi de la décomposition réduite des isométries avant d'attaquer le tableau de classification des isométries en dimensions 2 et 3.

On passe maintenant au chapitre II du plan. Une étude de type « groupe et topologie » des isométries, en fait, plus précisément, du groupe orthogonal. On donne la preuve (classique) que le groupe spécial orthogonal est engendré par des retournements.

3.1.55 Leçon 161-Distances et isométries d'un espace affine euclidien-2

On continue sur l'étude du groupe O_n, avec, d'une part les sous-groupes finis, qui se trouvent être, à conjugaison près, les sous-groupes finis de GL_n, *et* enfin l'indispensable apport de la topologie qui va nous amener à l'homéomorphisme de décomposition polaire et de la simplicité de SO_3. On clôt le chapitre avec l'apport des corps dans l'étude des isométries en dimension 2 et 3.

Nous voici rendu au chapitre III du plan sur l'optimisation des distances. Une affaire de goût bien entendu, mais qui nous amènera à des problèmes de compacité, d'extrema liés, calcul différentiel, et vers des problèmes de billards et de lois de la réflexion.

On s'attaque progressivement au problème du billard, en une bande, puis trois bandes, et on finit par parler du billard elliptique (en finissant par une référence). Dans les deux premières situations, on donnera une preuve utilisant la géométrie synthétique, qui utilise les symétries, et une autre avec la géométrie analytique, en utilisant le calcul différentiel et les extrema liés.

Voici le dernier volet sur la leçon 161. On parle de la distance à un convexe fermé, le point de Fermat, la distance d'une matrice au groupe orthogonal... On passe alors à des petites questions de jury dont le but est de tester quelques connaissances, mais surtout quelques réflexes.

3.1.56 Leçon 171-Formes quadratiques réelles, coniques, exemples et applications

Cette leçon est considérée comme « facile » pour le jury et « difficile » pour les candidats. Quel grand écart ! Peut-être le plus grand de toutes les leçons d'algèbre. Au programme : un 6 minutes, les peaux de bananes classiques, quelques questions de jury et une liste de développements possibles

3.1.57 Leçon 190-Méthodes combinatoires et dénombrement

Voici un petit aperçu des différents aspects du dénombrement tel que l'on peut le présenter à une leçon d'agrégation (et que l'on peut les trouver dans les carnets de voyage !). Tout d'abord, la définition du cardinal, puis trois aspects qui semblent essentiels à la leçon. *I*. Les parties d'un ensemble fini, muni de la réunion, de l'intersection... où il intéressant de présenter les différentes applications de la formule du crible, qui nous permet de déboucher sur des fonctions arithmétiques nommées par leurs lettres grecques. II. Le lemme du berger et la machine a créer du lemme du berger, j'ai nommé les groupes. On aboutit a la notion d'action de groupes, formule des classes et de Burnside. Enfin, III. la notion de séries génératrices qui débouche souvent (mais pas toujours) sur des problèmes d'analyse.

3.1.58 Leçon 190 - Questions de jury sur le dénombrement

Voici trois exercices classiques à l'agrégation qui illustrent trois types de méthodes déjà racontées sur cette chaîne, c'est-à-dire 1. opération sur les cardinaux-formule du crible, 2. Actions de groupes et formule des classes, 3. Utilisation des séries génératrices. 1. La décomposition de p^q en nombres binomiaux et nombres de Stirling 2. Le cardinal de l'ensemble des couples de sous-espaces supplémentaires dans un espace $\mathbb{K}^n$, où $\mathbb{K}$ est un corps de cardinal q. 3. Quelle est la dimension du sous-espace de $\mathbb{K}[X_1,\ldots,X_n]$ de polynômes homogènes de degré d.

3.1.59 Leçon 191 AE - Exemples d'utilisation de techniques d'algèbre en géométrie-1

3.1.60 Leçon 191 - Agrégation externe-Exemples d'utilisation de techniques d'algèbre en géométrie-2

On va parler plus précisément de cette leçon 191, et le bon ménage que constituent algèbre et géométrie. Dans un premier temps, on parle de l'algèbre linéaire : équations de variétés, utilisation du déterminant, réduction, application à la décomposition canonique en affine.

3.1.61 Leçon 191 - Agrégation externe-Exemples d'utilisation de techniques d'algèbre en géométrie-3

Toujours dans le cadre de la leçon 191. Voici que débarquent les formes quadratiques avec leur lot de coniques, quadriques, cônes d'Apollonius, et j'en passe

3.1.62 Leçon 191 - Agrégation externe-Exemples d'utilisation de techniques d'algèbre en géométrie-4

On s'intéresse ici aux nombreuses applications des groupes à la géométrie. On attaque d'abord l'utilisation de sous-groupes particuliers du groupe affine, avec le problème inverse des milieux. Ensuite, on parle de groupes d'isométries de solides platoniciens, et enfin de la recherche de sous-groupes finis de SO_3.

3.1.63 Leçon 191 - Agrégation externe-Exemples d'utilisation de techniques d'algèbre en géométrie-5

On insiste ici sur les groupes de transformation. On en donne rapidement le principe : se ramener par action de groupe, et à l'aide d'un invariant de préférence, à une situation plus simple d'un problème de géométrie, tout en préservant les invariants du problème. On en donne trois exemple avec comme invariants l'alignement/barycentre, la métrique, et enfin, la cocyclicité.

3.1.64 Leçon 191 - Agrégation externe-Exemples d'utilisation de techniques d'algèbre en géométrie-6

Voici le dernier volet de cette longue histoire. Il n'y aura ensuite plus qu'à faire son marché... On termine donc sur les complexes qui rendent plus digestes les similitudes du plan. Il y a des exemples à foison : théorème de Thébault, théorème de Napoléon, cocyclicité, foyers de l'ellipse de Steiner... Si à la place du plan, on veut travailler dans l'espace réel de dimension 3 ou 4, on se sert du corps de quaternions... Ensuite, on parle pêle-mêle de théorie des représentations, de théorie des corps et de la construction à la règle et au compas, de géométrie finie et de géométrie discrète...

3.1.65 Leçon 307 AI - Exercices avec utilisation de polynômes irréductibles 1

3.1.66 Leçon 307 AI - Exercices avec utilisation de polynômes irréductibles 2

3.1.67 Leçon 351 : Exercices avec utilisation de polynômes irréductibles-3

On utilise l'irréductibilité, dans le cas des polynômes réels cette fois, pour montrer que tout polynôme P de $\mathbb{R}[X]$ à valeurs positives sur $\mathbb{R}$ est somme de deux carrés de polynômes réels. Une espèce de « théorème des deux carrés » en mode polynomial.

3.1.68 Leçon 351 : Exercice avec utilisation de polynômes irréductibles-4

Cet exercice fait le lien entre degré de polynômes irréductibles et dimension de sous-espace stable. On montre que sur $\mathbb{R}$, un endomorphisme possède toujours un sous-espace stable de dimension inférieur ou égal à 2. Ceci est en lien avec le fait qu'un polynôme irréductible réel est de degré inférieur ou égal à 2.

3.1.69 Leçon 355 : Exercices faisant intervenir des automorphismes orthogonaux

On fait le point sur les nombreuses propriétés et caractérisations des matrices orthogonales qui leur permettent d'intervenir en algèbre linéaire (normes euclidiennes, normes subordonnées, décomposition polaire, décomposition QR, systèmes linéaires, topologie, actions de groupes, aires et volumes...)

3.1.70 Leçon 355 : Exercices faisant intervenir des automorphismes orthogonaux-2

Après avoir vu dans une première vidéo, les propriétés des matrices orthogonales, on présente deux exercices qui mettent, à eux deux, en avant les propriétés annoncées.

3.1.71 Leçon 154– Décompositions de matrices

On passe en revue toutes les décompositions de matrices à bien connaître pour un oral d'agrégation (décomposition polaire, Dunford, LU et QR). On en donne à chaque fois, les hypothèses, les résultats, les variantes, les applications et les algorithmes associés.
Oubli : je n'ai pensé qu'après coup de l'application de la décomposition QR à l'inégalité d'Hadamard...

3.1.72 Question de jury sur « Décomposition de matrices »

Un petit exercice de jury permet de tester une mine de petits savoir-faire en réduction !

3.2 Développements (77)

3.2.1 Algèbre linéaire

La décomposition LU par Patrick Sam Al Habobi

Patrick Sam nous présente la décomposition d'une matrice en une matrice triangulaire inférieure unipotente « L » et une matrice triangulaire supérieure « U ».
On continue sur des questions de jury. Il manque peut-être la question sur la complexité de l'algorithme.

Trace et Dualité par Laetitia

Laetitia nous présente le développement de Carnet de Voyage en Algébrie sur le thème trace et dualité. Chaud les questions ! bravo à elle pour sa super note à l'oral cette année !

Forme trace et dualité

On fait le point sur **la forme trace, vue comme une forme bilinéaire symétrique sur l'espace des matrices carrées. On explique, ici, pourquoi elle est non dégénérée et pourquoi cette propriété est essentielle pour comprendre plus finement l'algèbre de matrices $\mathrm{M_n(K)}$.**

3.2.2 Réduction

Le théorème de Kronecker

Voici **un développement assez classique : la preuve d'un théorème de Kronecker qui décrit les polynômes unitaires à coefficients entiers et dont les racines sont de module inférieur ou égal à 1. Ici, la preuve est axée sur la matrice compagnon**.

ENS ′86 Matrices de Moore (feat. théorème spectral... et la trace)

Voici un développement que l'on peut trouver dans « 30 développements pour l'agrégation de mathématiques » de Bastien Lartigue. On y trouve de la réduction, du théorème spectral et de l'arithmétique. Mieux, il possède une très belle interprétation en termes de théorie des graphes que l'on évoquera en épilogue.

Les tutos de la prépa : méthode de Newton pour la décomposition polaire par Antoine 1

Antoine nous propose un développement à cheval sur l'algèbre linéaire et l'analyse : une méthode de Newton pour calculer la décomposition polaire d'une matrice inversible réelle. A l'aide du théorème spectral, on se ramène au problème analogue en dimension 1, c'est à dire la méthode de Héron, ce qui ne nous rajeunit pas.

Les tutos de la prépa : méthode de Newton pour la décomposition polaire par Antoine 2

Le jury (Nicolas et Philippe) posent leurs questions à Antoine autour de son développement sur la méthode de Newton pour la décomposition polaire.

Le théorème de décomposition de Frobenius par Loïc

Loïc nous présente le théorème de décomposition de Frobenius qui nous dit qu'un espace muni d'un endomorphisme se décompose en sous-espace cyclique. Un développement sur la réduction des endomorphismes qui s'adapte bien à la leçon sur la dualité ainsi que la leçon sur les sous) espaces stables.

Le corps $\mathbb{C}$ est algébriquement clos par Martin

Martin exécute en 15 minutes chrono la preuve, par la réduction, du théorème de d'Alembert-Gauss (le corps des complexes est algébriquement clos) telle qu'on peut la trouver dans Carnet de Voyage en Algébrie I-3.27. Il s'ensuivra un petite dizaine de minutes de questions de jury sur ce beau développement !

Errata. Noté par loloolaf. Quand il est écrit $chi_u = P$ et pareil pour v, il faut plutôt prendre le polynôme minimal vu les degrés !

L'algorithme de Berlekamp

On présente le classique algorithme de Berlekamp qui permet de factoriser rapidement un polynôme de $\mathbb{F}_p[X]$ en facteurs irréductibles.

mais il est bon de voir les deux. Feat. Stella (la star !)

Réduction des automorphismes de Frobenius et de Berlekamp

On étudie l'automorphisme de Frobenius sous l'angle de la réduction et nous allons caractériser sa classe de similitude. Comme application, on construit un « multi-Frobenius », c'est-à-dire un morphisme de Frobenius composante par composante, et on montre comment la réduction de ce morphisme nous permet d'obtenir les degrés des composantes irréductibles d'un polynôme P de $\mathbb{F}_p[X]$.

Deux exercices sur Berlekamp

On propose deux polynômes à décomposer « à la main » en facteurs irréductibles par l'algorithme de Berlekamp. En fait on ne demandera ici que le degré des facteurs irréductibles.

Exercices sur la décomposition de Frobenius

Quelques petites questions autour de la décomposition de Frobenius.

Forme de Smith et application (à effet waouh !)

On présente ici la forme (normale) de Smith pour une matrice carrée A à coefficient dans un corps. Il s'agit d'une matrice diagonale portant sur sa diagonale les polynômes invariants de similitude de A. Après avoir montré l'existence d'une telle forme normale à partir du théorème de décomposition de Frobenius, on passe à une application ravissante, proposée par *stevie4ever* dans les commentaires de cette chaîne. Il propose une preuve alternative d'une preuve donnée sur cette chaîne que le quotient de χ_A par μ_A est le PGCD des coefficients de la comatrice de $XI_n - A$.

Nombre de matrices diagonalisables sur un corps fini par Mathis

Le retour de Mathis sur cette chaîne, en mode bidouilleur, pour nous parler du cardinal de l'ensemble des matrices diagonalisables de taille n sur un corps fini. La présentation se fait sous forme de développement et les questions de jury ne tardent pas à venir au bout des quinze minutes réglementaires.

3.2.3 Algèbre linéaire et topologie

Cayley-Hamilton topologique par Raphaël

Bravo à Raphaël qui vient de decrocher le concours ! Le voici au coeur de sa preparation en trai de présenter le théorème de Cayley-Hamilton dans sa version topologique de Carnet de Voyage en Algébrie Exercice 3. 42.

Adhérence des matrices diagonalisables réelles

Voici un développement assez agréable tiré de Carnet de Voyage en Algébrie, où l'on prouve que l'adhérence des matrices diagonalisables réelles est égal à l'ensemble des matrices trigonalisables réelles. Dans la foulée, on montre que sur $\mathbb{C}$, l'adhérence des matrices diagonalisables est l'espace des matrices tout entier.

Homéomorphisme de décomposition polaire (développement)

Tiphaine nous propose une preuve (issue, par exemple, : -), de Nouvelles histoires hédonistes de groupes et de géométries, chap. VI) de l'homéomorphisme de décomposition polaire.

L'homéomorphisme de décomposition polaire par RIri

Une présentation soignée de l'homéomorphisme de décomposition polaire face à un jury à l'affut !

Au passage, on pourra trouver une pléthore d'applications de cette décomposition sur `https://youtu.be/c0othDKgVeY`

Développement sur la décomposition polaire (par Dom)

Dom nous propose le développement classique sur la décomposition polaire. Il s'en suit une série de questions impitoyables du jury.

La suite de polygones par Caroline

Caroline nous présente, avec son flow stylé, le développement sur la suite de polygones du plan complexe (Carnet de Voyage en Algèbrie, 1. 3. 33). Au programme : réduction, convexité, barycentres, et limites de suites de matrices. Qui dit mieux ?

Sous-groupes bornés de GLn(C) par Mathis

Mathis aime bidouiller dans les sous-groupes bornés. Il va nous prouver en un développement (Oraux-X-ENS) qu'un sous-groupe borné non trivial de $\mathrm{GL}_n(\mathbb{C})$ ne peut pas être aussi petit que l'on veut (pour une norme subordonnée). En clair, il n'existe pas de groupe non trivial strictement inclus dans la boule de centre identité et de rayon $\sqrt{3}$. S'en suit une séance de question où on passe en revue les problèmes de normes subordonnées, de normes d'algèbres, le lien avec le spectre, la décomposition de Dunford multiplicative (mieux adaptée aux groupes) et des propriétés utiles des matrices nilpotentes. Rien que ça ! ! !

3.2.4 Analyse

La méthode d'Archimède par Caroline

Caroline, que l'on félicite pour son super classement à l'interne cette année, propose la méthode d'Archimède, face à un jury qui ne manque pas de questions. Pour ceux et celle qui veulent avoir un avant-goût de ce que certains agrégatifs appellent l'enfer lyonnais :˜)
Source : le Dantzer

Les nombres de Bell par Séverine

Séverine nous présente une formule donnant le n-ième nombre de Bell, c'est-à-dire le nombre de partitions d'un ensemble de cardinal n, dans sa version analytique. Le format est celui d'un développement et il s'en suit une petite séance de questions.

Fonction zeta sur les entiers naturels pairs par Caroline

La fonction zeta associe à s supérieur à 1 la somme des $1/n^s$. On sait souvent montrer en licence que l'image de 2 est le fameux $pi^2/6$. La généralisation de cette formule aux entiers pairs demande les nombres de Bernoulli, et plus généralement un mélange d'intégration de polynômes de Bernoulli et de décomposition en séries de Fourier.

Les tutos de la prépa : le théorème de Bohr-Mollerup par Audrey

Extrait de Carnet de Voyage en Analystan. On connaît la fonction gamma, essentielle en analyse complexe. Audrey en montre ici une caractérisation par la log convexité et son équation fonctionnelle $f(x+1) = xf(x)$. Il s'agit du théorème de Bohr-Mollerup. Audrey en profite des minutes d'arrêt de jeu pour en déduire la formule de duplication de Legendre.
S'en suivent quelques questions de jury (par Tewfik et Philippe). C'est le moment de montrer qu'on est en mode zéro bluff !

Les tutos de la prépa : le théorème de Riesz par Raphaël 1

Le théorème de Riesz dit que si E est un espace vectoriel normé de dimension infinie, alors la boule unité de E n'est pas compacte. Voici la preuve de Raphaël dans le plus pur exercice de style du développement à l'oral de l'agrégation.

Les tutos de la prépa : le théorème de Riesz 2

Après le développement de Raphaël sur le théorème de Riesz, voici le moment des questions du jury. Cela donne une bonne idée de comment les choses se passent le jour J.

Développement de la série harmonique

Le développement de la série harmonique est un bel exercice d'analyse qui peut se faire par étapes successives. Dans un premier temps, il y a l'apparition de la constante d'Euler, suivie dans un deuxième temps du calcul des premiers termes en $1/n$ et $1/n^2$. Mais pour obtenir un développement « illimité », il faut passer par les nombres de Bernoulli sur lesquels nous ne tarirons pas d'éloges.

Le théorème de Korovkin par Patrick Sam Al Habobi-1

Le théorème de Korovkin est un théorème d'approximation de fonctions sur un compact. Il permet de prouver une convergence uniforme d'une certaine famille de fonctions à partir de très faibles hypothèses.

Le théorème de Korovkin par Patrick Sam Al Habobi-2

Questions de jury sur ce développement

Le théorème de Korovkin et son application au théorème de Weierstrass

Voici un développement (en fait deux développements car il y a deux résultats) que l'on peut trouver tel quel dans Carnet de Voyage en Analystan. Le puissant théorème de Korovkin et son application au non moins puissant théorème de Weierstrass sur la densité des polynômes dans l'espace des fonctions continues sur un compact.

Irrationnalité de Pi par Riri

Dans cet état de calme mental affiché qui le caractérise, Riri nous présente une preuve de l'irrationnalité de Pi, que l'on peut trouver dans Carnet de Voyage en Analystan. Et, tout en s'élevant (par l'absurde) au-dessus de la hâte des hommes, il tient tout de même le pari d'exécuter ce développement en moins de 15 minutes !

Méthode de quasi-Newton par Patrick Sam Al Habobi-1

Dans le format d'un développement à l'oral de l'agrégation, Patrick Sam Al Habobi nous propose une méthode de quasi-Newton pour inverser une matrice réelle. Au programme : suites de matrices, méthode de Newton, théorème spectral et normes subordonnées. Référence : Carnet de voyage en Analystan.

Méthode de quasi-Newton par Patrick Sam Al Habobi-2

Dans le format d'un développement à l'oral de l'agrégation, Patrick Sam Al Habobi nous propose une méthode de quasi-Newton pour inverser une matrice réelle. On aborde ici la séance de questions sur le développement.

Les tutos de la prépa. L' équation différentielle $X' = AX1/2$

Avant d'attaquer le problème de l'allure et la stabilité des solutions des équations différentielles de type $X' = AX$, il est bon de faire quelques préliminaires et de passer à la loupe les outils usuels qu'exige la situation.

Les tutos de la prépa. L' équation différentielle $X' = AX2/2$

On donne une autre approche pour l'allure des courbes dans $\mathbb{R}^2$ solutions de l'équation différentielle $X' = AX$. Cette approche passe par une classification plus grossière que celle des classes de similitude (on s'autorise à multiplier par un scalaire non nul).

Courbes solution du système d'équations différentielles $X' = AX$ dans le plan réel par Aurélien

Aurélien présente un développement pour l'agrégation interne (ou externe). Il s'agit de classer toutes les situations possibles pour les courbes solutions de l'équation $X' = AX$ où A est une matrice réelle de taille 2. Il en suit quelques questions de jury.

Méthode des puissances par Patrick (développement et questions de jury)

Patrick Sam Al Habobi nous présente, sous le format de développement à l'agrégation (interne ou externe), la méthode des puissances pour l'approximation de valeurs propres d'une matrice symétrique réelle. On peut trouver ce développement dans une version récente de Carnet de Voyage en Analystan (publié chez l'IREM Lyon).
On continue avec une série de questions de jury
Une typo toutefois dans la récurrence, il faut lire $x_{n+1} = Sy_n$ au lieu de $x_n = Sy_n$.

Noyau de Fejér par Florence

Florence propose de nous parler du noyau de Fejér dans le cadre de la convergence des séries de Fourier. Il suivra de ce développement une petite séance de questions.

Preuve analytique de Cayley-Hamilton par Pat-Sam

Patrick Sam revient sur la chaîne pour une preuve de Cayley Hamilton par le calcul d'intégrales !

Une preuve analytique du théorème de Cayley-Hamilton

Voici une preuve analytique du théorème de Cayley-Hamilton sur le corps des complexes. Elle est toutefois montrée de manière élémentaire pour pouvoir en faire profiter à la fois à ceux qui ne connaissent pas la théorie de fonction holomorphes, et à ceux qui la connaissent et qui sauront en trouver des raccourcis. On passe par un jolie formule de résidus matriciels qui permet de définir, en général, l'analogue matriciel d'une fonction (analytique) complexe.

Entrelacement des solutions d'équations différentielles par Caroline

Et oui, les mathématiques peuvent aussi exprimer de la tendresse avec l'entrelacement de solutions d'équations différentielles. C'est Caroline, fraîchement agrégée, qui va nous le montrer au cours d'un développement que l'on peut trouver dans « Carnet de Voyage en Analystan » exercice 69 (version Calvage et Mounet)

Les nombres de Bell par Radia

Radia présente les nombres de Bell selon Carnet de Voyage en Analystan Exercice 37. NE changez rien aux réglages, on est bien en vitesse réelle !

Noyaux reproduisants et espace de Bergman par Guillaume

Guillaume propose un développement original pour l'agrégation : les espaces de Bergman dans le cadre des espaces de Hilbert à noyau reproduisant. Dans un premier temps, il installe la théorie avec ses définitions, ses exemples, ses propriétés et ses caractérisations, avant de passer à l'exemple de l'espace de Bergman. Au programme, espaces de Hilbert, théorème de Riesz, fonctions holomorphes...

Références : Pour la première partie de la vidéo sur les noyaux reproduisants, il suit un exercice du livre « Eléments d'analyse fonctionnelle » de Hirsch et Lacombe. Pour l'espace de Bergman, c'est inspiré du livre « Espaces de Hilbert et opérateurs » de Bayen et Margaria

Inégalité de Wirtinger/Inégalité isopérimétrique par Nina

Nina nous propose l'inégalité de Wirtinger et son application au problème d'optimisation de l'aire avec une longueur donnée ! La présentation se fait en mode développement de quinze minutes suivi d'une séance de questions.

Théorème de Weierstrass version probabiliste par Nina

Nina nous propose la preuve probabiliste (due à Bernstein) du théorème de Weierstrass et que l'on peut trouver dans Carnet de Voyage en Analystan. La présentation se fait en mode développement de 15 minutes avec les questions de jury qui ne manquent pas de suivre !

Zêta... par Nina !

Non, ce n'est pas le nouveau parfum de Nina Ricci ! En mode développement 15 minutes pour l'agrégation, Nina nous présente les propriétés classiques de la fonction zêta. Caroline (que l'on a eu le bonheur de voir sur la chaîne), et Julien se sont constitués en jury "d'anciens de la prépa" pour lui poser quelque question. Ambiance assurée !

3.2.5 Arithmétique

Critère d'Eisenstein par Laetitia

Laetitia nous présente le critère d'Eisenstein. Maintenant qu elle vient d obtenir l'agrégation avec une belle prestation à l'oral, on peut dévoiler les coulisses de la preparation.

Coprimalité, Moebius et Zêta par Arthur

Arthur et sa craie Excalibur viennent nous présenter un développement transversal sur les thèmes, dénombrement, arithmétique et probabilités. On montre que si l'on choisit au hasard deux nombres de 1 à n, la probabilité pour qu'ils soient premiers entre eux tend vers $6/pi^2$. Source : carnet de voyage en Analystan.
Errata : a `13:02`, dans la preuve du point 2 il faudrait remplacer la somme de d allant de 2 à n en une somme ou l'ensemble des diviseurs de d est dans P_n, avec d different de 1.

Le critère d'Eisenstein (et applications) par Marie

Marie nous présente ici le critère d'Eisenstein, en insistant sur le contenu de Gauss. Elle termine sur une application que l'on peut trouver avec bonheur dans carnet de voyage en Algébrie : -)

Théorème de progression arithmétique de Dirichlet (version faible)

Pour tout entier n strictement positif, on montre qu'il existe un nombre infini de nombres premiers congrus à 1 modulo n. On suit une preuve que l'on peut trouver dans Carnet de Voyage en Algébrie.

Résoudre un système de congruence par Caroline

Système de congruences tel qu'il est fait dans Carnet de Voyage en Algébrie, Exercice 4. 2. 8. Attention, on n'est pas dans la situation « premiers entre eux ».

Théorème de Sophie Germain par Julien

Julien le sérénissime nous présente ici le théorème de Sophie Germain sur l'équation de Fermat. J'ai tout essayé pour le démonter au moment de la séance de questions... rien n'y a fait !

Le test de primalité de Lucas-Lehmer

On introduit la suite L_n de Lucas-Lehmer et on montre que le nombre de Mersenne M_p est premier si et seulement si M_p divise L_{p-2}. On en donne une preuve qui utilise la loi de réciprocité quadratique et une variante sans son utilisation. Dans les deux cas cela nous fera un bon développement pour l'agrégation externe.

Lemme de Zolotarev- 2 est-il un carré modulo p ?

Le lemme de Zolotarev crée un lien entre le symbole de Legendre de a modulo p et la signature de la multiplication par a. Voici une brêche entre arithmétique et groupes de permutation !

La norme sur les corps finis

On présente dans cette vidéo les propriétés de la norme sur un corps fini. Tout d'abord sous la forme d'un développement proposé par Matthias Hostein sur son site
https ://perso.eleves.ens-rennes.fr/people/matthias.hostein/agreg.html
On part ensuite sur des considérations plus borderline comme le théorème de Chevalley-Warning et Hilbert 90.

Le nombre 26 par Luca

Luca, avec son aisance naturelle, nous parle de son développement à l'oral de l'agrégation mathématiques sur une équation de Mordell ! Il a encore dans sa mémoire vive, toutes les questions que le jury lui a posées :-)

3.2.6 Groupes

Les Tutos de la Prépa- le groupe du tétraèdre par Rozenn

Un beau développement sur le groupe du tétraèdre (Carnet de Voyage en Algébrie) parfaitement exécuté par Rozenn. Il s'en suit quelques questions classiques de jury.

SO (3) est simple, par Benjamin

Voici une méthode topologique, voir Carnet de Voyage en Algébrie 3. 5. 6, pour montrer que le groupe spécial orthogonal SO (3) est un groupe simple. L'exposé est donné par Benjamin en format « développement à l'agreg » (15 minutes ou peu s'en faut)
Questions de jury, à brule pourpoint.

Le groupe $SO_2(\mathbb{F}_p)$ par Clément

Clément nous présente un groupe orthogonal fini : le groupe des matrices orthogonales sur le corps fini $\mathbb{F}_p$ tel qu'on peut le retrouver dans Carnet de Voyage en Algébrie. On montre que ce groupe est cyclique, ce qui n'est finalement pas si étonnant pour un cercle, même sur un corps fini !

Nombre de solutions d'une équation dans un groupe fini et table de caractères-1

Luca propose le développement de **Nouvelle Histoires Hédonistes de Groupes et Géométries Tome 2, Chap. XIV-A.14. Soit G un groupe fini, on veut trouver, à l'aide de la table de caractères de G, le nombre de solutions d'une équation dans G^{k}, où l'on impose les g_{i} dans des classes de conjugaison fixées**.

Nombre de solutions d'une équation dans un groupe fini et table de caractères-2

Luca propose le développement de Nouvelle Histoires Hédonistes de Groupes et Géométries Tome 2, Chap. $XIV - A$. 14. Soit G un groupe fini, on veut trouver, à l'aide de la table de caractères de G, le nombre de solutions d'une équation dans G^k, où l'on impose les g_i dans des classes de conjugaison fixées.

Agrégation externe : Action de Steinitz sur les espaces de matrices

Un développement de Tiphaine (agrégative) sur l'action de Steinitz sur les matrices, et dont les orbites sont classifiées par le rang. Lorsque l'on est sur $\mathbb{R}$ ou $\mathbb{C}$, on peut comprendre les adhérences d'orbites pour cette action.

p-Sylow en situation géométrique

Nous partirons de cette constatation que les théorèmes de Sylow rappellent les théorèmes fondamentaux de la géométrie vectorielle (ou affine, euclidienne, etc) qui disent finalement que l'on a des systèmes maximaux standards (les bases, les repères, les bases orthonormées, etc), que ces systèmes maximaux sont reliés par un groupe (le groupe des automorphismes GL_n qui agit transitivement sur les bases) et que toute sous-partie peut s'injecter dans un système maximal standard. On montrera ici que les p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$ sont en bijection avec les drapeaux complets de $\mathbb{F}_p^n$.

Le collier de perle (version Kétrane)

Sam Patrick Al Habobi nous présente la version du collier de perles du Kétrane. On compte un nombre de colliers de perles modulo l'action du groupe diédral, avec un nombre fixé de perles de couleurs données. S'en suivent les questions de jury.

Sous-groupes de $\mathbb{R}$. L'alternative dense/monogène par Caroline

Un théorème essentiel pour l'approximation des nombres réels que nous présente Caroline, sous forme de développement à l'agrégation. Il est tiré de Carnet de Voyage en Algébrie.

S'en suivent la série de question de jury...

Volumes et décomposition polaire

Un petit développement pour l'utilisation de la décomposition polaire, cette fois-ci appliquée à la préservation des volumes. On refait ici la preuve de l'existence de la décomposition polaire pour une matrice (inversible ou pas).

3.2.7 Géométrie

Condition de cocyclicité de quatre points par Caroline

Voici un critère de cocyclicité de quatre points A, B, C, D : l'existence d'un quadruplet de réels non tous nuls a, b, c, d tels que pour tout point M, $aAM^2 + bBM^2 + cCM^2 + dDM^2 = 0$

Ellipsoïde de John-Loewner

Myriam nous présente l'ellipsoïde de John-Loewner. Un développement des plus transversaux, mais attention aux épines !

Une méthode express (et expresse) pour les isométries du cube

Une méthode classique pour comprendre le groupe des isométries du cube passe par son action sur ses quatre grandes diagonales. Ici, nous proposons une méthode qui consiste à passer par son action sur ses trois axes de symétrie. Cela a l'avantage d'obtenir de jolies matrices orthogonales. On donne la preuve dans un premier temps, puis, dans un épilogue, on voit comment récupérer des matrices pour l'hypercube et pour le tétraèdre.

Ellipse de Steiner par Caroline

Caroline revient nous présenter l'existence et l'unicité de l'ellipse de Steiner d'un triangle. S'en suit une petite séance de questions.

Optimiser l'aire d'un triangle inscrit dans deux cercles tangents

Sam nous présente un petit développement qui mêle savamment, cercles, triangles, géométrie, calcul différentiel, trigonométrie et topologie... Référence : le Karmati

Groupe orthogonal, points extrémaux et enveloppe convexe

Deux développements en une seule vidéo ! D'une part, on montre que l'enveloppe convexe de O_n est la boule unité B pour la norme subordonnée à la norme quadratique de $\mathbb{R}^n$. Et inversement, on prouve que l'on retrouve O_n comme l'ensemble des points extrémaux de la boule B.

Points remarquables du triangle et barycentres

Un exercice incontournable dans la leçon des barycentres est celui qui consiste à réaliser les points remarquables d'un triangle par ses coordonnées barycentriques. En voici un exposé qui fait à peu près le tour de la question.

Construction à la règle et au compas du p-gone régulier par Loris

Loris nous présente le développement complet sur la construction à la règle et au compas du p-gone régulier. Le développement est tout de même à réduire tout de même (on en parlera dans une seconde vidéo). On montre que le p-gone régulier est constructible si et seulement si $p = 2$ ou si p est un premier de Fermat, c'est à dire $p = 2^{2^n} + 1$ ($+p$ premier, ce qui n'est pas gagné).

Questions de jury-Règle et compas+ version galoisienne

A la suite du développement de Loris concernant la construction du p-gone régulier à la règle et au compas, on pose quelques questions de jury dont, en particulier, celle de la construction du n-gone régulier. *A* la suite de quoi, on proposera une version de Gauss-Wanzl pour ceux qui connaissent un peu la théorie de Galois.

3.2.8 Polynômes, anneaux, corps

Le théorème de Gauss-Lucas et application par Séverine

Un développement tiré de Carnet de Voyage en Algébrie (seconde édition). Le théorème de Gauss-Lucas affirme que si P est un polynôme complexe de degré supérieur à 2, alors les affixes des racines du polynôme dérivé P' sont dans l'enveloppe convexe des affixes des racines de P. Comme application, elle montre que si P'' divise P alors les racines de P sont toutes alignées.

Théorème de Gauss-Lucas et application- par Patrick Sam Al Habobi

Le théorème de Gauss-Lucas stipule que les affixes des racines de la dérivée d'un polynôme complexe (non constant) se situent dans l'enveloppe convexe des affixes des racines du polynôme. On va en déduire que si la dérivée seconde de P divise P, alors toutes les racines de P sont alignées.

Théorème de Gauss-Lucas et application-2

La séance de questions de jury ! Séance qui pourra en éclairer quelques uns sur la convexité.

Une tour de corps quadratique par Adam

Adam nous propose (pour la gloire de l'esprit humain) l'étude d'une extension du corps Q des rationnels par des racines carrées d'une famille de nombres sans facteurs carrés et deux à deux premiers entre eux. Il le fait sous la forme d'un développement à l'oral de l'agrégation et subit en conséquence un assaut de questions de jury !

3.2.9 Probabilités

Probabilité pour que deux éléments commutent dans un groupe fini

On cherche à exprimer la probabilité p_G que deux éléments tirés indépendamment dans un groupe fini G, de façon équiprobable, commutent entre eux. On va voir que si G est non abélien (ie p_G différent de 1), alors p_G ne peut pas dépasser 5/8, borne atteinte, par exemple, pour le groupe diédral et le groupe quaternionique. Mais on trouvera une formule particulièrement simple pour p_G mettant en relation l'ordre de G et le nombre de classes de conjugaison. Cet exercice figure dans Carnet de Voyage en Analystan.

Probabilité pour que deux matrices commutent dans $\mathrm{GL}_2(K)$

On vient de voir dans une vidéo précédente une formule simple qui relie ordre du groupe fini G, nombre de classes de conjugaison, et probabilité pour que deux éléments commutent dans G. On va donner une illustration de cette formule quand G est le groupe GL_2 sur un corps fini, ce qui va nous permettre d'utiliser nos connaissances sur la réduction !

Probabilité pour que deux matrices commutent dans $\mathrm{GL}_n(K)$

On vient de calculer la probabilité pour que deux matrices de $\mathrm{GL}_2(K)$ commutent sur un corps fini $\mathbb{K}$. La généralisation de ce résultat à $\mathrm{GL}_n(K)$ demande un peu plus de savoir et de savoir-faire. De savoir tout d'abord, avec le théorème de décomposition de Frobenius qui va trouver son objectif plein-emploi dans cette vidéo, et de savoir-faire avec des techniques classiques (mais manifestement souvent ignorées des étudiants à l'agrégation) de séries génératrices.

3.2.10 Formes quadratiques

Le critère de Sylvester par Geneviève

Geneviève nous propose un joli développement sur le critère de Sylvester, exécuté en temps réel (Si-si !). Il s'en suit une séance de questions autour des formes quadratiques réelles. Sources : Carnet de Voyage en Algébrie, *p.* 115

Critère de diagonalisabilité de Klarès par Florence

Un joli critère dans un format de développement pour montrer qu'une matrice sur $\mathbb{C}$ est diagonalisable sur une condition qui porte sur son commutant. Et bien sûr à la suite, la séance de questions de jury.

Diagonalisabilité : le critère de Klarès

Une preuve ravissante qui peut fournir un développement agréable dans le cadre d'une leçon sur la réduction ou sur les formes quadratiques. On peut le trouver dans le chapitre II de Carnet de Voyage en Algébrie.

L'ellipsoïde de John Loewner par Radia

Radia nous présente ici l'ellipsoïde de John et Loewner. Un développement riche dans la diversité de ses thèmes abordés (formes quadratiques, inégalité de Minkowski, volumes, théorème spectral, convexité...) et en corollaires (en particulier, la caractérisation des sous-groupes compacts maximaux de $\mathrm{GL}_n(R)$). On finit sur une conversation où Radia nous parle de sa passion des mathématiques.
Petit errata. Radia parle de forme quadratique en écrivant une norme à $5'50$ et $11'46$. il faudrait élever au carré pour que ce soit vraiment une forme quadratique

3.3 Questions d'oral (27)

3.3.1 Question de jury sur la leçon $106-$ Groupe linéaires-Sous-groupes

Voici une petite série de questions successives de jury qui passe en revue un bon nombre de points (pas tous évidemment, ce serait trop beau) dans cette leçon 106 sur le groupe linéaire et ses sous-groupes. On passe en revue, le groupe spécial linéaire, le sous-groupe des homothéties, les groupes à un paramètres, les problèmes d'engendrement et même les isomorphismes exceptionnels.

3.3.2 Questions de jury sur le thème racines de l'unité

Voici trois questions de jury sur la leçon 102 où l'on doit parler de racines de l'unité. Trois choses fondamentales sous-jacentes à ces questions. 1) L'utilisation de l'irréductibilité des polynômes cyclotomiques Phi_n sur Q et leur degré phi (n). 2) Le fait que phi (n) tend vers l'infini avec n. 3) le fait que pour étudier l'intersection de deux extensions, il est important de connaître le corps engendré par ces deux extensions.

3.3.3 Question de jury- Leçon PGCD ou rang-dimension

Un exercice posé au jury de l'interne cette année. Il s'agit de tirer des informations sur le pgcd de deux polynômes caractéristiques des matrices A et B à partir d'une matrice C de rang r qui vérifie $AC = CB$. Un futur classique ?

3.3.4 Question de jury sur le thème distances ou extrema

On trouve en algèbre comme en analyse, à l'inter comme à l'externe des leçons sur les distances ou sur les extrema. Voici une question de jury récemment entendue et rapportée par le sympathique Nicolas !

3.3.5 Questions de jury autour du rang en algèbre linéaire

Tout d'abord : deux questions de jury classiques au cours d'une leçon d'agrégation sur le rang. Une, sur la diagonalisabilité, et l'autre (plutôt esprit agrégation externe qu'interne) sur la stabilité du polynôme minimal par extension. Mais à la fin, une rencontre du troisième type : -) !
Dans un deuxième temps, quelques questions classiques sur les propriétés topologiques du rang
Et pour finir, une dernière question de jury autour des propriétés du rang, mais cette fois-ci le rang concerne les formes quadratiques sur un corps fini !

3.3.6 Exercice de jury sur les actions de groupes

Un petit exercice de jury est le bon réflexe est de dire pour commencer... « j'ai envie d'utiliser les actions de groupes ».

3.3.7 Question d'oral à l'agreg externe (Anneaux et corps) -1

Quelques questions de jury de plus sur les anneaux et les corps. Au programme, extension, degré, polynôme minimal, factorialité, PGCD-PPCM, polynômes symétriques élémentaires, polynômes cyclotomiques modulo p...

3.3.8 Question d'oral à l'agreg externe (Anneaux et corps) -1bis

L'injection du groupe $\mathrm{GL}_n(\mathbb{F}_p^2)$ dans $\mathrm{GL}_{2n}(\mathbb{F}_p)$ est totalement naturelle et pourtant elle a été assez mal comprise, si j'en crois les retours de ceux qui ont visionné la vidéo 1. J'essaie d'expliquer que tout repose ici sur « l'oubli » que $\mathbb{F}_p^2$ est un corps, en se concentrant uniquement sur sa structure de $\mathbb{F}_p$-espace. C'est peut-être dans ce lâcher prise que réside toute la difficulté...

3.3.9 Question d'oral à l'agreg externe (Anneaux et corps) -2

Ici, il sera question de polynômes annulateurs d'un entier algébrique, irréductibilité, et donc critères par le degré d'une extension, et surtout le théorème de la base télescopique. On verra comment le phénomène d'unicité d'une extension de degré fixé dans le monde des corps finis, fait que le polynôme irréductible trouvé sur $\mathbb{Z}$ se décompose modulo p pour tout p. On passera ensuite en revue les corps algébriquement clos à connaître pour l'oral.

3.3.10 Question d'oral à l'AE (Anneaux et corps) -3

Un dernier pour la route (de l'oral). **Des polynômes cyclotomiques, la limite de la fonction indicatrice d'Euler, un lemme de Gauss pour les extensions de corps et son application au maintien de l'irréductibilité d'un polynôme par extension**.

3.3.11 Question de jury : Sous-anneaux principaux de Q

On résout cet exercice classique de montrer que tout sous-anneau de Q est principal.

3.3.12 Question d'oral à l'agreg externe (Réciprocité quadratique) −1

Toujours dans la série des questions de jury. Quelles sont les thèmes développés autour de la réciprocité quadratique ?

3.3.13 Question d'oral à l'agreg externe (Réciprocité quadratique) −2

On regarde plus particulièrement le développement de la loi de réciprocité quadratique par les formes quadratiques (il faut rendre à César ce qui appartient à César). On le regarde dans ses petits détails que pourraient questionner un jury, et dans ses extensions.

3.3.14 Question d'oral à l'agreg externe (Groupes finis) −1

On va s'intéresser aux petites questions de jury autour des groupes finis. Dans ce premier volet, on s'intéresse particulièrement aux groupes abéliens finis, et leur rapport, via le théorème de structure, à l'arithmétique des nombres. En suite, toujours lié au théorème de structure, l'omniprésence des groupes cycliques nous entraîne vers l'étude des homomorphismes entre $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$. C'est un véritable exercice de synthèse où se mêlent une pléthore de techniques à bien connaître sur les groupes (annulateurs, réciproque de Lagrange dans le cas cyclique, passage au quotient).

3.3.15 Question d'oral à l'agreg externe (Groupes finis) −2

Cette fois-ci on se concentre sur les actions de groupes (finis) sur des ensembles finis, qui donnent lieu à des propriétés arithmétiques (divisibilité) prêtes à être exploitées. On travaille en particulier sur les p-groupes et les p-Sylow.

3.3.16 Question d'oral à l'agreg externe (Groupes finis) −3

Ici, on s'intéresse à des petits problèmes de commutation dans le groupe des permutations. Ils se règlent en général à coup de « formule de conjugaison ». On traite aussi de la question de l'étude de S_4 et ses p-Sylow.

3.3.17 Question d'oral à l'agreg externe (Groupes finis) −4

On mélange les plaisirs avec des exercices transversaux demandant des techniques de groupes finis (Lagrange, formule des classes...) et réduction (trigonalisation, diagonalisation, matrices compagnon, polynômes d'endomorphismes...). Bref, on étudie certains sous-groupes de $\mathrm{GL}_n(\mathbb{F}_p)$.

3.3.18 Question d'oral à l'agreg externe (Algèbre linéaire) –1

On donne des petits exemples de questions de jury en insistant sur la façon dont ces questions peuvent être présentées. On est partis sur une série sur le thème (ouvert dense) de l'algèbre linéaire.

3.3.19 Question d'oral à l'agreg externe (Algèbre linéaire) –2

On regarde de plus près les propriétés de la comatrice. Tout d'abord, on va aller plus dans le cas particulier de la matrice carré A de rang $n-1$. On sait que com (A) est de rang 1, mais comment caractériser les coefficients de proportionnalité dans la comatrice ? Ensuite, nous discutons de petits problèmes afférents : trouver det (com (A)), com (com (A)), résoudre com $(A) = A$. A chaque fois, face au jury, l'abordage du problème par les cas extrémaux (A nulle, A inversible) est un bon moyen de négociation.

3.3.20 Question d'oral à l'agreg externe (Algèbre linéaire) –3

Quelques questions de jury pour tester des réflexes sur les problèmes de dimensions d'espaces vectoriels.

3.3.21 Question d'oral à l'agreg externe (Algèbre linéaire) –4

Voici une petite liste d'exercices pour s'entraîner sur la dualité. Il faut arriver dans cette leçon avec une solide notion du rôle de l'orthogonalité dans les transformations d'un problème vers un « problème dual », une fois sur deux, plus facile à résoudre.

3.3.22 Question d'oral à l'agreg externe (Algèbre linéaire) –5

On pose des petits exercices sur les endomorphismes diagonalisables en insistant sur une panoplie de réflexes à avoir. Parfois les problèmes de multiplicités algébriques et géométriques peuvent aider, mais ce sont surtout l'aide des polynômes d'endomorphismes qui va nous sauver dans des situations difficiles.

3.3.23 Question d'oral à l'agreg externe (Algèbre linéaire) –6

On continue sur le thème de petits exercices de jury sur les matrices diagonalisables en lien avec le critère du polynôme annulateur scindé simple. Précision utile à l'attention d'El Perforateur (merci à lui !), mais aussi pour les autres : dans la preuve où on veut montrer que M diagonalisable implique A nul, on prend mu (polynôme minimal de M forcément scindé simple), alors, Xmu et Xmu' annulent A. Donc X (pgcd des deux) annule A et A est nul.

3.3.24 Question d'oral à l'agreg externe (Algèbre linéaire) –7

Voici des petites questions de jury autour du thème « réduction et topologie ». Beaucoup de choses s'articulent autour du fait que l'application qui, à une matrice carrées complexe A, associe son polynôme caractéristique, est continue. La densité des matrices diagonalisables (en complexe !) est un incontournable du genre.

3.3.25 Question d'oral à l'agreg externe (Algèbre linéaire) -8

On continue sur les petites techniques de topologie en réduction. On commence avec les deux contre - exemples clef à bien connaître et ce qu'ils impliquent topologiquement. Ensuite, on disserte sur ce schéma classique qui consiste à étudier un problème lié à la réduction : 1. sur $\mathbb{C}$, 2. sur ses matrices diagonales, 3. sur ses matrices diagonalisables et enfin, sur $\mathcal{M}_n(\mathbb{C})$ tout entier.

3.3.26 Question d'oral à l'agreg externe (Algèbre linéaire) -9

Au programme du jour : les matrices nilpotentes. Il y sera abordé les aspects « invariants de similitude », topologie, dénombrement sur corps fini, critères par les drapeaux, et cotrigonalisation.

3.3.27 Question d'oral à l'agreg externe (Algèbre linéaire) -10

Dans cette dernière vidéo en algèbre linéaire, on se prépare à une question emblématique de la leçon sur les sous-espaces stables (réputée difficile). Pour cela, on observe comment le lemme des noyaux peut nous aider, à l'aide d'une propriété (et on n'insistera jamais assez sur le caractère exceptionnel de la distributivité) du lemme des noyaux, et de deux situations extrêmes sur les sous-espaces stables d'endomorphismes nilpotents.

3.3.28 exp(AB) vs exp(BA)

Un petit exercice de jury autour de l'exponentielle de matrices ?

3.3.29 Question d'oral à l'agreg externe (arithmétique)

Deux petits exercices étonnants autour d'une leçon sur les anneaux factoriels. Un qui illustre une application de l'anneau factoriel $\mathbb{Z}[i]$, et l'autre, plus simple est un application du critère d'irréductibilité d'Eisenstein.

4 Divertissements mathématiques (133)

4.1 Arithmétique

4.1.1 Exercice coup de coeur sur une suite récurrente linéaire

Une suite qui part de 2023 et qui peut nous occuper toute l'année ! si on en croit le résultat final. Un exercice coup de coeur très progressif proposé par Pascal Corm, qui utilise des techniques de collège dans un premier temps, puis, de licence, et enfin, de master puisqu'il nous emmènera dans le monde merveilleux des corps finis où tout élément non nul est une racine de l'unité. Merci Lagrange !

4.1.2 Un petit exercice d'arithmétique (équation diophantienne)

Un tout petit exercice d'arithmétique que m'a proposé mon ami Rached Mneimné sur la somme des carrés d'entiers consécutifs.

4.1.3 Cinq fois cinq vingt-cinq ou les rimes dans la table de multiplication

Cinq fois cinq vingt-cinq, six fois six trente-six mais sept fois sept ne font pas quarante-sept. Comment ça a pu partir comme ça en cacahuète ? En partant de la poésie des tables de multiplications de notre enfance, on arrive à la résolution de l'équation $x^2 = x$ modulo 10^k, en passant par le lemme chinois, l'indicatrice d'Euler, pour finir par des projecteurs de $\mathbb{Z}/n\mathbb{Z}$.

4.1.4 Nombres premiers et carrés consécutifs (on répond aux auditeurs !)

A la suite de la vidéo
`https://youtu.be/e2yjFyDE1No`
Arthur Meyer s'est interrogé dans un commentaire sur l'existence de nombres premiers p tels qu'il existe suffisamment de carrés consécutifs modulo p. Voici un petit exercice corrigé qui répond à la question, parce que c'est tellement rare d'avoir réponse à une question que c'est un plaisir de la donner ! : -)
sur la musique de (the answer my friend is) Blowing in the wind

4.1.5 Nombre de carrés consécutifs modulo p par Polya et Vinogradov

L'inégalité de Polya-Vinogradov permet de donner une borne au nombre de carrés consécutifs dans le groupe $\mathbb{Z}/p\mathbb{Z}^*$. Au programme : somme de Gauss et plus généralement anlayse de Fourier discrète (que l'on pourrait appeler « algèbre de Fourier » !)

4.1.6 Cinq preuves coup de coeur pour une infinité de nombres premiers !

On propose 5 preuves, toutes d'horizons totalement différents, pour l'infinitude de l'ensemble des nombres premiers (et la bravitude de leurs auteurs !)

4.1.7 Devinez la caractéristique du corps !

Un petit exercice taquin pour occuper nos méninges ! Soit a_i, i de 1 à 27 des éléments non nuls d'un corps $\mathbb{K}$. On suppose que la suite b_i, des sommes des a_j pour j différent de i, est une permutation des a_i. On doit montrer que cela n'est possible (et que ça l'est effectivement) pour certaines caractéristiques de $\mathbb{K}$.

4.1.8 Le p-adique (ses merveilleuses applications)

L' épreuve 1 de l'agrégation interne 2023 nous invite (maladroitement, certes) à nous intéresser aux entiers p-adiques. Nous allons introduire de façon pietonne les entiers et les nombres p-adiques, ainsi que de merveilleuses applications (empruntée à un article de Bruno Winckler) qui nous convaincrons que la théorie est indispensable.

4.1.9 Minoration de la fonction pi de comptage des nombres premiers (Capes 2008)

Le problème de CAPES 2008 nous a concocté une belle surprise. Un problème astucieux où une méthode d'approche de la fonction $pi(x)$ du cardinal de l'ensemble des nombres premiers inférieurs à x est proposée à l'aide de la simple fonction bêta. Bref, un bagage de terminale avec juste dans la boîte à outils intégration sur un segment et théorème fondamental de l'arithmétique, mais un résultat respectable !

4.1.10 Majoration de la fonction pi de comptage des nombres premiers (Capes 2008)

Après avoir minoré la fonction pi de comptage des nombres premiers, voici venu le moment de la majorer. Cela fait au final un joli problème de CAPES où l'on voit qu'on obtient un encadrement de la fonction pi à peu de frais.

4.1.11 Entiers consécutifs avec/sans facteurs carrés ?

Tout est dans le titre. Peut-on trouver des suites d'entiers consécutifs (avec/sans) facteurs carrés aussi longues que l'on veut.

4.1.12 Doctor Fibonacci, I presume ?

Un petit exercice, proposé par notre ami Denis Roussillat, sur les suites récurrentes de niveau terminale pré-Blanquer, et qui constituera une excellente alternative au Sudoku des plages.

4.1.13 Une (petite) identité de Ramanujan

On montre une identité arithmétique due à Ramanujan. Cette identité peut constituer un bel exercice sur l'indicatrice d Euler, ou sur les racines de l'unité.

4.1.14 Théorème de progression arithmétique : une preuve en 10 minutes ?

Après avoir donné tout récemment la preuve de Serre pour le théorème de progression arithmétique de Dirichlet, il n'est peut-être pas inutile d'en faire un résumé succinct afin d'en dégager les points forts.

4.1.15 Un tour de magie (avec des nombres binaires !)

Nous recevons la visite de notre ami Antoine qui nous propose un tour de magie avec les nombres binaires.

4.1.16 Le théorème de meilleure approximation rationnelle

On présente le théorème de meilleure approximation d'un réel par une fraction rationnelle. Pour le résumer, on pourrait dire que la « rentabilité » de l'approximation d'un réel a, par une fraction rationnelle p/q, est le rapport entre $a - p/q$ (en valeur absolue) et $(1/q^2)$. Legendre a montré en 1798 que si cette rentabilité est strictement plus petit que $1/2$, alors p/q est un terme de la suite de fractions continues qui converge vers a.
On prouve ensuite le théorème de meilleure approximation d'un réel par une fraction rationnelle.

4.1.17 $x^2 = x$ modulo 10^k ou les rimes de la multiplication

Cinq fois cinq vingt cinq, six fois six trente six mais sept fois sept ne font pas quarante-sept. Comment ça a pu partir comme ça en cacahuète ? En partant de la poésie des tables de multiplications de notre enfance, on arrive à la résolution de l'équation $x^2 = x$ modulo 10^k, en passant par le lemme chinois, l'indicatrice d'Euler, pour finir par des projecteurs de $\mathbb{Z}/n\mathbb{Z}$.

4.1.18 $\zeta(2)$ - Les plus belles preuves !

La formule qui affirme que la somme des $1/n^2$ vaut $pi^2/6$ est bien connue de tous les mathématiciens. Après avoir motivé les troupes, on se lance dans un florilège de preuves célèbres plus jolies les unes que les autres que l'on peut retrouver (pour certaines) sur `https://www.math.cmu.edu/~bwsulliv/basel-problem.pdf`

4.1.19 Des formules non polynomiales pour les nombres premiers !

On présente ici deux formules explicites amusantes, une formule donnant le n-ième nombre premier, et une autre formule donnant le nombre de nombres premiers plus petits que n.

4.1.20 Des formules polynomiales pour les nombres premiers ?

On donne tout d'abord deux méthodes pour prouver que l'ensemble des nombres premiers est infini. Point de départ d'une quête deux fois millénaire.

4.1.21 Une preuve d'Erdos sur la localisation des nombres premiers

Un petit exercice fortement inspiré de « *A* fun number theory problem » de Dr Barker, nous donne prétexte à donner la preuve assez ignorée (mais non moins brillante, venue du cerveau fertile de Paul Erdös, à 18 ans) d'un théorème célébrissime d'arithmétique que l'on peut résumer ainsi : « Chebychev said it, and *I* say it again, there is always a prime between n and $2n$ ».

4.1.22 Distribution des puissances en base 10 et loi de Benford

Encore un pan extraordinaire de l'histoire des mathématiques : la loi de Benford et le critère de Weyl. On peut en trouver des bribes introductives dans Carnet de Voyage en Algébrie, chap. III.

1. Peut-on justifier la loi de Benford qui prévoit la distribution de chiffres en base 10 dans une suite de nombres ? On va le faire dans une série de vidéos en partant de la suite des puissances de 2, on continue avec celle des puissance de 3, sans oublier les nombres de Fibonacci. Pour l'instant, pas de preuve, mais un premier énoncé.

2. La loi de Benford que l'on a pu observer sur quelques suites comme 2^n, 3^n, et la suite de Fibonacci, n'est pas un loi vraie en général pour toutes les suites. Dans cette vidéo, on formalise cette loi en la ramenant à des propriétés dans un espace de fonctions continues par morceau. C'est le début d'une voie royale vers une jolie théorie qui sera abordée dans la vidéo qui suit.

3. On part donc d'une suite de réels que l'on ramène à une suite de réels de $[0,1[$ (quitte à retirer la partie entière). On introduit le critère de Weyl qui caractérise les suites équidistribuées, c'est-à-dire les suites a_n telles que si A est un intervalle et 1_A sa fonction caractéristique, la moyenne des $1_A(a_k)$ pour k de 1 à n, tend vers la mesure de A. Ce critère demande tout simplement que pour tout s positif, la moyenne des exp $(2s\pi a_k)$, k de 1 à n, tend vers 0.

4. Après avoir prouvé le critère de Weyl dans la vidéo précédente, on se propose de fixer un petit cadre pour la loi de Benford, ce sera le cadre de certaines suites géométriques, qui se généralise sans peine au cadre de certaines suites linéaires récurrentes, comme la suite de Fibonacci.

5. On termine ce volet sur la loi de Benford en « rebondissant sur le billard ». En effet, la suite nlog (2) correspond à des rebondissement d'une boule sur un billard circulaire. On passe alors à un billard torique, pour voir que l'on peut, pour tout chiffre t, trouver un n tel que 2^n et 3^n commencent simultanément par t, avec le critère de Weyl multidimensionnel. En revanche, 2^n et 5^n commencent simultanément par t si et seulement si $t = 3$. Par exemple, si $n = 5$, on a à la fois $2^n = 32$ et $5^5 = 3125$.

4.1.23 Presqu'entiers et nombres de Pisot

Partie I. On va s'intéresser aux suites géométriques de réels dont les termes sont des « presqu'entiers » à partir d'un certain rang. On aboutit à une définition des « nombres de Pisot ».

Partie II. On va présenter, en tentant de motiver, la théorie de Charles Pisot. Tout d'abord en montrant l'utilité de ces nombres dans l'approximation diophantienne. Ensuite, en montrant que ces nombres sont à la fois rares (et donc chers), de par une caractérisation via les suites géométriques de presqu'entiers, et en même temps suffisamment présents dans la nature, puisque toute extension algébrique réelle de Q est engendrée par un nombre de Pisot.

Partie III. Les mathématiciens confirmés connaissent par coeur la formule du déterminant de Vandermonde, mais peu d'entre eux savent inverser la matrice de Vandermonde. Une astuce qui utilise les polynômes permet de le faire élégamment. On aura ensuite besoin de cette inversion pour montrer le théorème de Pisot dans une prochaine vidéo.

Partie IV. On prouve le théorème de Pisot. Un nombre algébrique réel supérieur à 1 qui est la raison d'une suite géométrique presque entière est un nombre de Pisot. La preuve est instructive et utilise pas mal de classiques de l'agrégation externe (théorème de Cayley-Hamilton, système de Vandermonde, sous-réseaux de $\mathbb{Z}^n$, morphisme de multiplication dans un anneau, morphismes de conjugaison dans un corps).

4.1.24 Le théorème de Fermat de taille moyenne 1

Qui pouvait se douter que l'on puisse attaquer à l'équation de Fermat modulaire à l'aide du simple principe des tiroirs ? Certainement un immense mathématicien comme Issaï Schur ! Voici, coincé entre le (trop) petit théorème de Fermat et le (trop) grand, prouvé par Andrew Wiles, le théorème de Fermat de taille moyenne. Une belle histoire de Noël, pour les grands et les petits...

4.1.25 Le théorème de Fermat de taille moyenne 2

On montre que pour un entier strictement positif k fixé, l'équation de Fermat $x^k + y^k = z^k$ possède une solution modulo p premier, pour p assez grand. Il s'agit là d'une preuve purement combinatoire, n'utilisant aucun (ou presque) ingrédient de la théorie des nombres.

4.1.26 Rudiments de théorie de Minkowski pour l'agrégation

On sait d'expérience que la théorie de Minkowski a rebuté plus d'un étudiant, tant son approche diffère des approches habituelles. Pourtant, le jeu en vaut la chandelle, dès que l'on veut assurer l'existence d'un point entier dans une partie de $\mathbb{R}^n$. Voici une présentation minimaliste de la théorie.

4.1.27 Un fractal de Pascal

Pour cette fin d'année, voici un petit aperçu d'une preuve de la structure fractale de triangle de Pascal, vu modulo p premier. Pour $p = 2$, nous avons le fameux triangle de Sierpinsky, mais pour les autres ? Dans un premier temps, nous voyons que le triangle modulaire cache une auto-similarité tensorielle...

On prouve ensuite la propriété d'auto-similarité tensorielle du triangle de Pascal modulo un nombre premier p, qui donnera dans une prochaine vidéo la structure fractale du triangle de Pascal. On montre en particulier que cette propriété repose essentiellement sur le morphisme de Frobenius, et donc, n'a que peu de chance de se généraliser tel quel pour tout entier n (non premier) et même pour toute puissance de p.

Puis, l'auto-similarité se fait fractale. Il suffit pour cela d'étendre le triangle vers l'intérieur au lieu de la faire vers l'extérieur. On s'intéresse donc aux fractales, qui auraient pu être mieux exploitée durement le confinement, en créant des kilomètres de parcours de santé dans un périmètre restreint. On présente (assez modestement) la structure fractale du carré de Pascal et du triangle de Pascal modulo p. On calcule facilement la dimension fractale de la jolie « structure triangle », par invariance, en la calculant sur la structure carrée (moins jolie mais forcément plus pratique).

4.1.28 Divine proportion, nombre plastique et méthode des puissances

Une construction classique consiste à partir d'un rectangle et lui associer un autre rectangle en plaçant un carré sur son côté. En itérant cette méthode (et en normalisant) on obtient à la limite le fameux rectangle d'or. On fait ici le lien entre cette construction et la méthode des puissances en algèbre linéaire, bien connue (oupa) des agrégatifs.

On cherche une « divine proportion en dimension 3 », pour faire plaisir aux architectes, mais également pour mettre à profit la méthode des puissances. Cette fois-ci, il faut résoudre l'équation $X^3 - X - 1$ dans le corps des complexe. On en profite pour montrer comment le discriminant permet de voir le nombre de solutions de l'équation. On tente de faire un lien de parenté entre nombre d'or et nombre plastique, pour tomber sur la notion de suite géométrique presqu'entière. On verra plus tard que ces deux nombres appartiennent à une famille remarquable de nombres réels : les nombres de Pisot.

4.1.29 Le théorème à la fin heureuse - la preuve de Paul Erdös

Un joli problème dans le plan affine qui donné naissance à une solution élégante de Paul Erdös, une théorie (et pas la moindre, la théorie de Ramsey), et un mariage...

4.1.30 Le théorème de Skolem-Mahler

Le théorème de Skolem-Mahler parle des zéros d'une suite récurrente linéaire entière. Il peut se faire avec les entiers p-adiques, mais l'épreuve de 2023 admettait un théorème un peu lourd de zéros isolés dans le cas p-adique, ce qui est, on l'admettra, bien dommage. On reprend ici la preuve du problème, mais on donne une preuve plus complète qui n'utilise que le corps des rationnels.

4.1.31 Seuls deux nombres en sandwich entre un carré et un cube !

Quels sont les nombres entiers situés « en sandwich » entre un carré et un cube. Selon si le carré est en dessous et au dessus, ce problème nous amène à étudier deux équations diophantiennes, dites de Mordell. Une, relativement classique en master, qui repose sur la factorialité de $\mathbb{Z}[i\sqrt{2}]$. Et une autre qui nous amène à l'anneau $\mathbb{Z}[i\sqrt{6}]$, qui malheureusement n'a plus cette belle propriété. Heureusement, Dedekind, Kummer sont passés avant nous et on défriché le terrain avec la notion de groupe de classes d'idéaux. Dans la théorie des nombres, les mathématiciens ont fini par trouver le partenaire idéal !

4.1.32 Factorisez $X^{16} - X$ en irréductibles sur le corps à deux éléments

Un exercice instructif qui nous oblige à bien maitriser la théorie des corps finis.

4.1.33 Factorisez $X^{16} - X$ en irréductibles sur le corps à deux éléments - 2

Voici une autre méthode instructive pour factoriser un polynôme sur un corps fini. On a besoin ici d'un théorème, qui fournit un joli développement, qui donne des renseignements précieux sur la décomposition des polynômes cyclotomiques en irréductibles.

4.1.34 Sous-espaces stables et idéaux de $\mathbb{K}[X]$

Un exercice élégant qui part du dénombrement de sous-espaces stables d'un espace E muni d'un certain endomorphisme et aboutit à une étude de l'arithmétique des polynômes.

4.1.35 5 est-il un carré modulo p ?

Nous venons de voir dans une vidéo précédente que 2 est un carré modulo p (différent de 2) si et seulement si p est congru à 1 ou -1 modulo 8. Nous allons voir une méthode très analogue qui nous montre que 5 est un carré modulo p (différent de 5) si et seulement si p est congru à 1 ou -1 modulo 5. Pour finir, nous verrons que cette approche nous fait découvrir au loin, tel un sommet enneigé, un immense théorème : le théorème de Kronecker-Weber.

4.1.36 $x^3 + 7$ peut-il être un carré ?

Encore un petit exercice d'arithmétique dont nous donnerons deux méthodes. Une, élémentaire (l'utilisation du petit théorème de Fermat en est le point culminant) mais très astucieuse, et une autre, qui utilise la factorialité et la connaissance des unités de certains anneaux d'entiers quadratiques.
Errata de FMA Arlandar : dans la seconde méthode, $2 = (3 + \sqrt{7})(3 - \sqrt{7})$ donc 2 se décompose comme un produit de deux premiers contrairement à ce qui est dit mais si un de ces deux facteurs premiers divisait $y + \sqrt{7}$ et $y - \sqrt{7}$ le second diviserait aussi les deux facteurs par conjugaison donc 2 diviserait les facteurs $y + -\sqrt{7}$ ce qui est impossible.

4.1.37 Le témoin de Solovay-Strassen - Un test de primalité

On présente un test élégant de primalité dû à Solovay et Strassen. On sait que le symbole de Legendre d'un entier a modulo un nombre premier impair p est égal à $a^{(p-1)/2}$. Quand on généralise par multiplicativité le symbole de Legendre à tout entier impair p, alors, on voit que cette égalité n'est plus vraie dès que p n'est pas premier. On peut donc utiliser cette propriété comme critère de primalité.

4.1.38 La loi de réciprocité d'Artin - 1

Il est tentant de généraliser la loi de réciprocité quadratique aux degrés supérieurs. C'est Emil Artin qui va donner un résultat pertinent, mais en commençant par modifier l'énoncé de réciprocité, par l'énoncé d'Euler de « loi de périodicité quadratique ». En quelques vidéos, je propose de raconter une petite partie de l'évolution, de Euler à Artin, en passant par Legendre et Gauss, de cette loi de réciprocité, au coeur de l'arithmétique et tout particulièrement, de la théorie du corps de classes.

4.1.39 La loi de réciprocité d'Artin - 2

On prouve le théorème de réciprocité quadratique d'Artin qui tient compte de la périodicité proposée par Euler, mais en y ajoutant un morphisme de groupe. Résultat, on construit un morphisme du groupe multiplicatif $(Z/4dZ)^*$ vers le groupe $1, -1$ qui envoie un nombre premier p ne divisant pas $4d$ vers le résidu quadratique de d modulo p.

4.1.40 La loi de réciprocité d'Artin - 3

On va regarder de près deux exemples clés : un dans le cas quadratique, et un autre en degré 3. Dans les deux cas, on constate la possibilité de relever l'automorphisme de Frobenius dans une extension de Q. Mais on a besoin pour cela de deux hypothèses : 1) partir d'un polynôme f sur $\mathbb{Z}[X]$ dont le groupe de Galois est abélien, et 2) partir d'un nombre premier p qui ne divise pas le discriminant de f.

4.1.41 La loi de réciprocité d'Artin - 4

On termine ce volet avec deux versions, dues à Artin, de la loi de réciprocité quadratique en degré supérieur. Une version pour les polynômes unitaires sur $\mathbb{Z}$, et une version pour les entiers de corps de nombres, qui nous amène à construire le « ray class group ».

4.1.42 Le lemme d'Artin ou l'invitation à la théorie de Galois

Le lemme d'Artin constitue un joli développement qui peut se placer dans des leçons comme systèmes linéaires, rang et dimension... et surtout extensions de corps. Voici sous une forme standardisée de quinze minutes un exposé sur ce lemme, sa provenance et ses conséquences.

4.1.43 Le théorème (fort) de progression arithmétique de Dirichlet

Le feuilleton (arithmétique) de l'été. On tente ici malgré la canicule de fournir une version motivée (et on l'espère, motivante) de la preuve de Jean-Pierre Serre du théorème de progression arithmétique de Dirichlet : si a et m sont premiers entre eux, il existe une infinité de nombres premiers congrus à a modulo m. Cerise sur le gâteau : une petite clause d'équidistribution. Merci à vct nll de nous avoir suggéré de parler de ce joli problème qui mêle caractères et analyse complexe.

4.1.44 Irréductibilité dans $\mathbb{Z}[X]$ par congruences

Une situation classique où l'on veut montrer qu'un certain polynôme à coefficients entiers est irréductible sur $\mathbb{Z}$. On utilise pour cela des décompositions modulaires (modulo p) de ce polynôme en irréductibles, et on compare les partitions des degrés obtenues afin de prouver l'irréductibilité du polynôme de départ. On en profite pour répondre à une question de Ludo sur `https://les-mathematiques.net/vanilla/index.php?$p=/discussion/2334895/comprendre-le-lien-entre-deux-questions#latestnews`
Errata : Juste à la fin il aurait fallu dire que a n'est pas multiple de p.

4.1.45 Les menteurs de Miller-Rabin - test de primalité

Voici un test de primalité réellement efficace ! Il s'agit du test de Miller-Rabin qui dit que si n est un entier impair non premier, une certaine batterie d'équations dans $(Z/nZ)^*$ n'a que très peu de solutions, alors que tout élément est solution si n est premier. Pour voir si n est premier, on prend un certain nombre d'éléments au hasard dans $(Z/nZ)^*$, et si un élément ne vérifie pas une équation, n n'est pas premier. Mais peut on être sûr que n est premier si tous les nombres choisis ont passé le test ? Y a-t-il des menteurs ?

4.1.46 Les nombres pseudo-premiers de Perrin - 1

Voici, présentée sous forme de problème à l'agrégation interne, la jolie suite de Perrin, qui semble fournir un test de primalité. On va voir que si p est premier, alors le terme u_p de la suite est divisible par p. On a longtemps cru que la réciproque était vraie... Attention, comme le fait remarquer Maticawa (merci à lui !) 341 n'est pas un nombre de Carmichael, c'est juste un nombre tel que $2^341 - 2$ est divisible par 341. Le premier nombre de Carmichael est 561.

4.1.47 Les nombres pseudo-premiers de Perrin - 2

On achève la preuve du fait que p premier implique que le p-ième terme de la suite de Perrin est divisible par p. On le montre par deux méthodes : une méthode plutôt « licence » qui utilise les relations coefficients-racines, et une méthode plutôt « master » qui utilise le morphisme de Frobenius en caractéristique p.

4.1.48 Les nombres pseudo-premiers de Perrin - 3

On s'intéresse à la ressemblance entre nombres de Fibonacci et nombres de Perrin. En quoi sont-ils cousins ? Bien entendu, les relations de récurrence se ressemblent, mais on va chercher d'autres ressemblances dans leur réalisation en tant que nombres de parties d'un ensemble.

4.1.49 Les nombres pseudo-premiers de Perrin - 4

On arrive à un moment particulièrement agréable où l'on a réalisé que les nombres de Perrin se réalisent comme cardinal d'un ensemble de parties stables par le groupe cyclique. La formule des classes va nous donner une troisième preuve du critère de (pseudo) primalité de Perrin. On profite de cette grande cousinade pour inviter à la table les nombres de Lucas, qui se réalisent eux aussi comme cardinal d'un ensemble de parties stables par le groupe cyclique.

4.1.50 Lemme du ping-pong et groupe modulaire

Le lemme du ping-pong et son application au groupe modulaire constituent une illustration édifiante de ce que les actions de groupes peuvent apporter à l'étude du groupe lui-même. Dit autrement, l'adage « dis-moi sur qui tu agis et je te dirais qui tu es » est ici parfaitement représenté dans le cadre du groupe le plus célèbre de l'arithmétique : le groupe modulaire.

4.1.51 Application de la cyclicité de $(\mathbb{Z}/p\mathbb{Z})^*$: les nombres de Giuga

Une petite application sympathique au développement de la cyclicité du groupe $(Z/pZ)^*$, pour p premier ? Une nouvelle famille de pseudos premiers : les nombres de Giuga. Et celle-ci est particulièrement coriace puisque, d'après Paulo Rimbenboim dans son « Book of prime numbers records », 1700 chiffres significatifs n'arrivent pas à invalider la conjecture.

4.1.52 Le problème des sabliers d'Euclide

Un petit problème de sablier, de niveau élémentaire, qui demande tout de même un peu d'astuce, et qui n'est pas sans rappeler un algorithme bien connu : -)

4.1.53 Le problème des pièces de monnaies de Frobenius

Le problème des pièces de monnaie que nous présentons ici se ramène au problème de comprendre de la partie additive dans N engendrée par deux nombres premiers entre eux. La solution proposée par Frobenius est à la fois simple et admirable ! Et en plus, à la fin, il y a un (Fro) bonus ! ! !

4.1.54 Le corps $\mathbb{C}$ est algébriquement clos. Ma preuve coup de coeur !

Le théorème de d'Alembert-Gauss raconté aux enfants de Galois. Au programme, un peu de théorie de Galois, groupes de Sylow, propriétés classiques des p-groupes et... le TVI !

4.1.55 Théorème de Kronecker. La preuve la plus simple ?

Voici, à un niveau où le pré-requis serait le programme de master (on va dire, à un niveau « agreg externe »), ma preuve préférée du théorème de Kronecker, classique parmi les développements à l'oral, qui dit que tout polynôme unitaire de $\mathbb{Z}[X]$ ayant des toutes ses racines de normes inférieures ou égales à 1, possède des racines soit nulles soit racines n-ième de l'unité.

4.1.56 Polynômes symétriques vs invariants de Dickson (Maths en Hamac)

Un dernier épisode estival de maths en hamac pour parler d'une preuve d'une élégance rare des théorèmes classiques sur les polynômes symétriques (ils sont engendrés par les polynômes symétriques élémentaires qui sont algébriquement indépendants). Non seulement élégante, mais aussi généreuse, cette preuve s'applique également aux invariants de Dickson que l'on réintroduira ici. On montre alors que ces invariants sont algébriquement indépendants et qu'ils engendrent l'algèbre des $\mathrm{GL}_n(\mathbb{F}_q)$-invariants de $\mathbb{F}_q[X_1, ..., X_n]$.

4.1.57 L'équation de Fermat par Kummer (the hamacless version !)

L'équation de Fermat a fait tant d'émules que je ne me pouvais me contenter d'une version orale à distance de hamac. Voici une preuve rigoureuse (modulo quelques sauts quantiques) du théorème de Kummer qui dit que l'équation $x^p + y^p = z^p$ n'a pas de solution non triviale dans $\mathbb{Z}$ si p est un premier régulier. Ici, on ne se contente pas de traiter le "cas facile" (lol) où p ne divise pas xyz, mais on donnera aussi une idée de la preuve dans le cas où p divise xyz.

4.1.58 Groupe de Galois et réduction modulo p

Une énigme sur les groupes de Galois consiste à comprendre pourquoi on peut injecter le groupe de Galois d'un polynôme P de $\mathbb{Z}[X]$ quotienté modulo p dans le groupe de Galois de P. Voici une méthode que je trouve convaincante dans sa démarche, qui consiste à prendre un peu d'élévation, travailler sur un anneau de polynômes à plusieurs indéterminées qui permet de concilier les deux mondes.

4.1.59 Une formule de récurrence simple pour les nombres premiers

Je présente une formule étonnante d'Éric Trefeu, mathématicien amateur, une formule simple à la fois dans son énoncé et dans sa preuve. D'une part, je donnerai une version du crible d'Eratosthène par les séries génératrices, puis, j'en déduirai une formule de récurrence élégante (mais théorique) qui donne un nombre premier en fonction de ses prédécesseurs. Dans une première partie, nous nous adressons aux mathématiciens amateurs ou aux jeunes passionnés qui voudraient contacter un expert en mathématiques, afin qu'ils évitent des erreurs classiques de communication.

4.1.60 Du nouveau sur les morphismes de l'espace des polynômes !

Béranger Seguin, algébriste, chercheur, et viewer de la chaîne à ses heures perdues, a écrit un petit article que l'on peut trouver sur la plateforme Arxiv, où il étudie les endomorphismes d'une algèbre de polynômes vérifiant des propriété de conservation liées à la multiplicité des racines. Un exercice de haut vol dont j'ai extrait un résultat intéressant avec une compilation de belles idées.

4.1.61 Le dernier théorème de Fermat pour p régulier (Maths en Hamac)

L'équation de Fermat $x^n + y^n = z^n$ n'est plus à présenter et nous allons en voir ce que l'on pourrait appeler son (avant-)dernier rebondissement : le résultat de Kummer sur le cas où n contient un facteur premier régulier. Et, face à un problème nécessitant une telle élévation, quoi de mieux que d'en parler sans les mains et à hauteur de hamac ?

4.1.62 Des nombres puissants (et un échange stupéfiant)

Dans le cadre de la fête de la science, on décrypte une conversation entre Paul Erdös et Kurt Mahler, deux mathématiciens de haut vol, qui a eu lieu à Oslo en 1936, et qui portait sur les nombres puissants.

4.1.63 Une conique pour la loi de réciprocité quadratique !

Ça vous plairait, un voyage en conique avec une escale dans chaque corps ? C'est Bruno Winckler qui a écrit cette petite perle pour prouver la loi de réciprocité quadratique et que je présente ici...

4.1.64 La table des restes de J^3

Jean-Jacques Juré m'a envoyé son article que je présente ici, où l'on trouvera avec bonheur (et nostalgie !) une table des restes permettant de travailler avec des collégiens et des lycéennes autour d'une méthode par les graphes du calcul du reste dans une division euclidienne. Ma contribution est de montrer ici que ces tables de restes peuvent être éclairantes dans l'enseignement supérieur.

4.1.65 Conjecture de Goldbach-version polynomiale !

La conjecture de Goldbach joue encore des tours à ceux qui veulent s'y attaquer voir par exemple le théorème de Marguerite. Pourtant cette conjecture est si simple quand on la regarde dans le contexte des polynômes : soit A un polynôme unitaire à coefficients dans Z, alors il est somme de deux polynômes irréductibles à coefficients dans Z. Essayez pour voir... :-)

4.2 Groupes

4.2.1 Exercice Oraux X-ENS : quand le groupe d'automorphismes d'un groupe est-il trivial ?

Un exercice donnés aux oraux X-ENS et présenté par Luca Castelli. Trouver tous les groupes G tels que $Aut(G)$ est réduit à l'identité. Cet exercice peut paraître surprenant, mais Luca nous va nous faire la lumière sur ce problème.

4.2.2 Un 2-Sylow de S_4 en 6ème avec l'IREM

Je propose de présenter ici une de mes fiches « Galion » de sixième. On apprenait les groupes à cette époque, et je trouve admirable le travail de l'IREM pour faire passer ce que l'on appelait les maths modernes. On finit avec un peu de recul sur les maths de master qui se cachent derrière cette fiche. Mais tout de même, quelle utopie extraordinaire en cette fin des trente glorieuses.

4.2.3 Décimales et groupes cycliques- le nombre 142857 et ses amis

Voici un petit tour de magie, à la Gérard Majax, qui fait intervenir groupes cycliques et décimales.

4.2.4 Les théorèmes de Sylow dans un carré

Il est toujours instructif de voir ses théorèmes abstraits à travers le prisme de la géométrie. Ici, nous proposons de voir les théorèmes de Sylow via l'action du groupe des isométries du carré sur les sommets de ce même carré.

4.2.5 Le pfaffien, la pfabuleuse histoire ! (racontée par Pfil)

Découvrir le pfaffien est une expérience marquante. On se retrouve partis vers une belle histoire où les diverses composantes des mathématiques viennent s'entraider autour d'un théorème profond aux multiples avatars. On y trouvera le déterminant (développement de Laplace), les actions de groupes, les formes quadratiques et leurs classifications, les groupes de Lie... On aboutit à d' exceptionnels isomorphismes !

4.2.6 Surjectivité du morphisme de $\mathrm{SL}_n(\mathbb{Z})$ vers $\mathrm{SL}_n(\mathbb{F}_p)$

Construire le morphisme de $\mathrm{SL}_n(\mathbb{Z})$ vers $\mathrm{SL}_n(\mathbb{F}_p)$ est une chose aisée. Mais prouver qu'il est surjectif demande un certain savoir-faire !

4.2.7 Critères de simplicité d'Iwasawa pour un groupe $-1/2$

Qui aurait pu prévoir un lien entre simplcité d'un groupe et multi-transitivité d'une action fidèle ? Et bien Iwasawa a ouvert une voie royale entre les deux notions. On montre dans une première vidéo un lemme préliminaire, puis, un critère de simplicité pour un groupe à action multi-transitive à stabilisateur simple. Et c'est simple... comme bonjour !

4.2.8 Critères de simplicité d'Iwasawa pour un groupe $-2/2$

Qui aurait pu prévoir un lien entre simplcité d'un groupe et multi-transitivité d'une action fidèle ? Et bien Iwasawa a ouvert une voie royale entre les deux notions. On montre dans une première vidéo un lemme préliminaire, puis, un critère de simplicité pour un groupe à action multi-transitive à stabilisateur simple. Et c'est simple... comme bonjour !

4.2.9 Galois et la non résolubilité par radicaux

Comment Evariste Galois a pu prouver cette non résolubilité par radicaux de certains équations en degré 5, la où *Leonhard'Euler* s'était cassé les dents ? Et puis pourquoi 5 d'abord ? On fait le point détaillé sur les étapes de sa preuve qui consiste à transvaser le problème en un problème sur les groupes finis.

4.2.10 Le nombre 20160 et un non-isomorphisme exceptionnel - 1

20160, 196884, et quelques monstres... Nous allons aujourd'hui parler de coïncidences numériques, et en particulier, parmi les ordres des groupes simples. Dans le prochain volet, on montrera ce scandaleux résultat que, malgré les indices et les apparences, les deux groupes simples $\mathrm{GL}_3(\mathbb{F}_4)$ et $\mathrm{GL}_4(\mathbb{F}_2)$ ne sont pas isomorphes.

4.2.11 Le nombre 20160 et un non-isomorphisme exceptionnel - 2

On montrera ce scandaleux résultat que, malgré les indices et les apparences, les deux groupes simples $\mathrm{GL}_3(\mathbb{F}_4)$ et $\mathrm{GL}_4(\mathbb{F}_2)$ ne sont pas isomorphes. Il faut profiter de ce nombre 20160, parce qu'il n'y en aura pas d'autres comme cela avant 4. 585. 351. 680.

4.2.12 Le théorème de Polya sur les coloriages

Colorier un ensemble fini X revient à fournir une application de cet ensemble vers un ensemble K de couleurs. Si G est un groupe fini qui agit sur X, on rappelle comment calculer le nombre de coloriages modulo l'action de G. On montre ensuite le théorème de Polya qui établit une formule synthétique pour les coloriages modulo G ayant un nombre prédéfini d'éléments de couleur donnée.
Errata : Aux alentours de $20'30$ ", je me prends les pieds dans le tapis entre le nombre d'orbites de cardinal j et la suite de la taille des orbites...

4.2.13 Le théorème de Cartan-Von Neumann

Le théorème de Cartan Von Neumann (ou tout simplement de Cartan) dit qu'un sous-groupe fermé du groupe $\mathrm{GL}_n(\mathbb{R})$ possède une structure de sous-variété de $\mathcal{M}_n(\mathbb{R})$. On va passer un peu de temps à prouver et commenter ce théorème, mais quand on en voit la puissance, on se dit que ce n'est pas du temps perdu !

4.2.14 Fibration de Hopf (par les quaternions)

I'm pickin' up good fibrations it's giving me the excitations (oom bop bop)
Petits calculs entre amis dans le corps des quaternions. On part d'une magnifique animation des chapitres 7 et 8 de « Dimensions » en cherchant à en comprendre les calculs sous-jacents. Afin de simplifier à l'extrême les calculs, nous allons réaliser cette fibration à travers une action de la sphère quaternionique sur les imaginaires quaternioniques !
Elle est déjà dans la vidéo, mais je me fends de deux liens
Dimensions 7 et 8 `https://www.youtube.com/watch$?$v=tX_NUlO_tbw` `https://www.youtube.com/watch$?$v=ECHNPCTLL8c`

4.2.15 Etude du groupe de Rubik

Cette vidéo propose la lecture d'un article qui étudie le cube de Rubik d'un point de vue de la théorie des groupes. On donnera une description du groupe à partir de l'analyse du cube, puis on en décrira le centre, les éléments d'ordre 2, et on découvrira que certains sous-groupes classiques y sont cachés. Au programme, actions de groupes, produits semi-directs, hyperplans, et même action par homographie !

4.3 Analyse

4.3.1 L'exponentielle expliquée à mon voisin Nico

Je réexplique, avec force détails et illustration, ma vidéo récente sur l'exponentielle et le logarithme à mon voisin Nico, actuellement en thèse d'économie, et qui m'a fait entendre sa frustration de ne pas comprendre son contenu... La chaîne, qui s'adresse ici plutôt à un autre public, ne perd pas de sa saveur !

4.3.2 Prix Abel 2024 (autour d'une question elliptique)

Le prix Abel 2024 a été décerné au mathématicien Michel Talagrand. Nous en profitons pour parler d'une mystérieuse définition dans les travaux d'Abel : le terme « intégrale elliptique d'Abel ». Comment du latin « ellipsis » (omission, manque), nous en sommes venus à définir l'ellipse, l'intégrale elliptique, et enfin les courbes elliptique ? PS : merci à Fanny pour le bandana, sans lequel cette vidéo n'aurait pas été possible ! : -D

4.3.3 Prix Abel 2025- L époustouflant Masaki Kashiwara !

C'est le mathématicien Masaki Kashiwara qui a obtenu le prix Abel 2025 ! Je me permets donc de donner un petit aperçu de ses résultats les plus prestigieux (qu'il me pardonne la vulgarisation terre à terre de sa pensée transcendante !)

4.3.4 Théorème d'inversion de Lagrange et nombres de Catalan

Comment inverser un développement limité ; on parle de l'inverse pour la composition des fonctions et non pas pour la multiplication ! La formule peut être assez simple... à condition que la fonction soit facile à inverse, mais cette fois-ci pour la multiplication. Bref, c'est la formule d'inversion de Lagrange qui sera prouvée avec le calcul complexe. On en donnera ensuite une application classique au dénombrement des arbres binaires.

4.3.5 La balade de Narayana

Nous présentons ici les nombres de Narayana que l'on calcule grâce à des séries génératrices et la formule d'inversion de Lagrange.

4.3.6 Pourquoi Log et Exp sont inverses l'une de l'autre ?

Si on définit l'exponentielle et le logarithme par leur série entière, comment montrer élégamment qu'ils sont inverses l'un de l'autre ? Nous allons en faire la preuve à l'aide du groupe symétrique... Et oui, les groupes sont partout !

4.3.7 Fonctions absolument continues par Tristan

Voici le troisième et dernier volet de vidéos proposées par Tristan autour du théorème fondamental de l'analyse. Dans le second volet, on avait vu que l'escalier du diable proposait une fonction continue dérivable presque partout, qui toutefois ne vérifiait pas l'égalité, devenue habituelle depuis Newton, sur le lien entre fonction et intégrale de la dérivée. C'est l'absolue continuité qui va nous permettre d'éviter ce genre de contre - exemples monstrueux. On reviendra pour finir sur les fonctions lipschitziennes.

4.3.8 L'escalier du diable par Tristan

Tristan nous a parlé du problème de représentation de Riesz pour une fonction lipschitzienne, c'est-à-dire représenter $f(y) - f(x)$ sous forme d'une intégrale de x à y. Maintenant, serait-il suffisant d'avoir f continue dérivable presque partout et $f'L^1$ pour obtenir une représentation de f comme intégrale de sa dérivée ? L'escalier du diable, qui porte bien son nom, vient détruire cet espoir à tout jamais.

4.3.9 Peut-on couper un gâteau (polygonal) en 6 parts égales avec trois coups de couteau ?

Une petite histoire extraite du livre très recommandable de Pascal Boyer « Algèbre et géométries ». Une solution étonnante à ce problème très concret, qui utilise le TVI dans tous ses états.

4.3.10 Le corps $\mathbb{C}$ est algébriquement clos, par les intégrales de Cauchy.

On peut juger de l'efficacité de l'analyse complexe, et en particulier du théorème d'intégration de Cauchy par sa façon de trivialiser la preuve du théorème de d'Alembert-Gauss.

4.3.11 Théorème de représentation d'une fonction lipschitzienne par Tristan

Tristan nous propose un théorème haut en couleur qui prouve que toute fonction lipschitzienne u sur $\mathbb{R}$ peut être représentée par une fonction g dans $L^{infty}(R)$ dans le sens : $u(y) - u(x) = \int_x^y g(t)$ dt.

4.3.12 Le théorème de Borsuk-Ulam ou la rencontre des pôles-1

Peut-on trouver à chaque instant sur terre deux points antipodiques avec exactement la même température et la même pression ? Et bien, aussi contre-intuitif que cela puisse paraître, la réponse est « spoiler alert ». En tout cas, le théorème de Borsuk-Ulam nous confirme tout cela en toute dimension. Nous allons donc parler de ce théorème en dimension 1 dans la vidéo 1, puis en dimension 2 dans la vidéo 2 !

Errata : je dis que Borsuk Ulam est une seule et même personne mais n en est rien. ce sont bien deux mathématiciens distincts. En revanche Art et Tatum sont la main gauche et la. main droite du même pianiste `:-)` Comme quoi, les musiciens sont les meilleurs !

4.3.13 Le théorème de Borsuk-Ulam ou la rencontre des pôles-2

Peut-on trouver à chaque instant sur terre deux points antipodiques avec exactement la même température et la même pression ? Et bien, aussi contre-intuitif que cela puisse paraître, la réponse est « spoiler alert ». En tout cas, le théorème de Borsuk-Ulam nous confirme tout cela en toute dimension. Nous allons donc parler de ce théorème en dimension 1 dans la vidéo 1, puis en dimension 2 dans la vidéo 2 !

4.3.14 Le théorème de Fejér prouvé par Korovkin

Une suggestion de mon ancien étudiant Luca Castelli : la théorie de Korovkin permet de voir que les fonctions trigonométriques sont denses dans l'espace des fonctions continues périodiques (pour la norme uniforme). La théorie de Korovkin a cela de merveilleux que la preuve ne demande que de montrer qu'un certain opérateur est positif, qu'il est à valeurs dans les fonctions trigonométriques, et que $u_n(f)$ converge uniformément vers f, pour $f = 1$, cos et sin ! Référence : Hirsch-Lacombe p. 33.

4.3.15 Les projecteurs spectraux par l'analyse complexe

Un étudiant de licence de mathématiques a rencontré les projecteurs spectraux, les même qui permettent de montrer le lemme des noyaux. Toutefois, il les a, en général, vu dans le contexte de l'arithmétique avec l'identité de Bezout. Voici une autre approche qui utilise la formule des résidus en analyse complexe. Dans les deux approches, une seule idée : le passage du local au global.

4.3.16 Un paquet cadeau, c'est pour offrir !

On veut montrer qu'un compact convexe X de $\mathbb{R}^n$ peut être « empaqueté » dans un hypercube circonscrit (chaque face touche X et X est inclus dans l'hypercube). La preuve pour $n = 2$ ne demande finalement que le théorème des valeurs intermédiaires. La preuve pour $n = 3$ nous permet de dévoiler la puissance des groupes d'homotopie. On présentera au passage le fameux principe de l'assiette à soupe.

4.3.17 La conjecture de sensitivité par Corentin Faipeur-1

La conjecture de sensitivité parle de l'unification de la mesure de complexité des fonctions booléennes ; thème particulièrement pertinent en informatique théorique. Corentin Faipeur nous parle de ce qui est devenu désormais le théorème de Huang, après plus de trente années de résistance.

4.3.18 La conjecture de sensitivité par Corentin Faipeur-2

Après avoir motivé la conjecture, Corentin définit les différentes mesures de complexité d'une fonction booléenne, complexité elle-même garante de sécurité. Il y a la sensitivité par blocs, la sensitivité, et enfin, le degré total de la fonction vue comme polynôme à plusieurs variables. On veut montrer que toutes ces mesures sont « équivalentes » pour une équivalence à définir. C'est là que le récent théorème de Huang intervient. Il ne reste plus qu'à le démontrer dans une prochaine vidéo.

4.3.19 La conjecture de sensitivité par Corentin Faipeur-3

On prouve le théorème de Huang, qui démontre la trentenaire conjecture de sensitivité à l'aide du théorème d'entrelacement de Cauchy ainsi qu'une petite astuce basée sur une matrice d'adjacence « au signe près ». Pour le théorème d'entrelacement, on pourra se référer à `https://youtu.be/47ycHzMVIp8`

4.3.20 Le théorème ergodique de Von Neumann (version discrète)

Voici la version discrète du théorème de Von Neumann, dans sa version « prête au développement » que l'on peut trouver dans Objectif Agrégation.

4.3.21 Nombre de carrés consécutifs modulo p par Polya et Vinogradov

L'inégalité de Polya-Vinogradov permet de donner une borne au nombre de carrés consécutifs dans le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$. Au programme : **somme de Gauss et, plus généralement, analyse de Fourier discrète** (que l'on pourrait appeler "algèbre de Fourier" !).

4.4 Polynomes

4.4.1 Pinceau de polynômes scindés

Clément de Seguins Pazzis a récemment mis un post sur mathematiques. net
`https://les-mathematiques.net/vanilla/discussion/2337412/pinceau-de-polynomes-scindes-`
`latestnews`
où il est question d'une famille de polynômes scindés à un paramètre sur un corps fini. Cela fait un joli exercice sur les polynômes (avec au menu, PGCD, identification de fonctions polynômes sur corps finis, vandermonde...) avec une preuve élégante.

4.4.2 Localisation des racines d'un polynôme (une brève histoire)

On présente ici quelques résultats clefs sur la localisation des racines d'un polynôme réel en fonction des coefficients de celui-ci. Tout d'abord, la borne de Gauss, devancée par la borne de Cauchy. Ces généralités étant faites, on attaque le théorème de Enestrom-Kakeya, ses corrollaires ainsi que ses développements plus récents.

4.4.3 Localisation des racines d'un polynôme-addendum

Suite à une remarque de Toto, voici une preuve instantanée du théorème qui dit que si un polynôme réel non nul possède des coefficients croissants, alors ses racines sont de module dans le disque unité. Cette preuve est particulièrement agréable car elle utilise l'algèbre linéaire.
Scoop de *Toto*[2] : on peut trouver la preuve dans le livre « Petit compagnon des nombres et de leus applications » de Pascal Boyer *p.* 349 (avec la matrice compagnon, on pouvait s'y attendre !)

4.4.4 Une devinette polynomiale

Une devinette que m'a proposée Daniel Juteau où l'on doit deviner un polynôme en deux questions ! Alors qu'on ne sait même pas son degré !

4.4.5 La formule de Jacobi-Trudi (par le lemme de Gessel-Viennot) −3

Parmi les bases de polynômes symétriques, la plus convoitée est celle des polynômes Schur pour leurs liens avec la théorie des représentations (de GL_n et de S_n), la calcul d'intersection, la cohomologie, etc... On va présenter les formules de bases de cette famille de polynômes, à l'aide du tout petit (mais vaillant !) lemme de Gessel-Viennot.

4.4.6 Gessel-Viennot, l'approche alternative du déterminant

On a montré dans une vidéo précédente que l'on pouvait présenter de façon combinatoire le déterminant d'une matrice extraite du triangle de Pascal. `https://youtu.be/nWTXmncGZV4`
On a utilisé pour cela l'étonnant lemme de Gessel-Viennot qui est rentré dans les lemmes de légende avec le lemme de Gauss, de Fatou, de Burnside... On montre comme ce petit lemme permet de comprendre en profondeur les aspects combinatoires du déterminant.

4.4.7 Identité de Vandermonde en dimension supérieure

Ulysse Serres (que je remercie vivement au passage !) m'a récemment parlé d'un article de mon collègue Itaï Ben Yaacov « the Vandermonde identity in higher dimension » `https://arxiv.org/abs/1405.0993`, dont je présente le résultat fondamental. Curieusement, c'est une version dualisée de la matrice de Vandermonde qui se généralise le mieux ! au final, on déduit de cette identity une jolie propriété sur l'annulation d'une famille d'hyperplans.

4.5 Maths et musique

4.5.1 Les tonalités musicales vues par un mathématicien-1

Surtout que le mathématicien en question est MONSIEUR Michel Broué, et j'avais à coeur de partager son article que vous pouvez télécharger sur sa page web

4.5.2 Les tonalités musicales vues par un mathématicien-2

4.5.3 Les tonalités musicales vues par un mathématicien-3

4.6 Divers (inclassables)

4.6.1 Remarquables identités

On passe en revue tous nos souvenirs de troisième et de seconde, où nous avions rencontré pour la première fois les identités remarquables. Mais avec le recul, nous pouvons les voir désormais comme des formules de congruences entre formes quadratiques ! Tout un programme. Au final, nous ferons la lumière sur une identité remarquable relativement méconnue, mais liée à résultat fondamental de Grothendieck-Witt sur la diagonalisation des formes quadratiques par congruence !

4.6.2 Changement d'heure (et dualité)

Heure d'hiver, heure d'été ? On avance l'heure, ou on la recule ? On dormira un peu plus ou on manquera de sommeil ? Ce dernier week-end de mars où l'on passe à l'heure d'été est propice à ce genre de questionnement. On en profite donc pour remettre les pendules à l'heure en faisant le point sur la dualité !

4.6.3 Des voeux de bonne année avec Hilbert-2024 !

Il n'est jamais trop tard pour découvrir les bienfaits des polynômes de Hilbert, qui ont d'ailleurs fait l'objet des épreuves écrites de l'externe en 2021. Merci à Denis pour la suggestion !

4.6.4 Les invités du Capitaine Woody

Un petit quizz autour d'un problème mondain lors d'une croisière sur le paquebot du Capitaine Woody.

4.6.5 Une preuve sans mot (relativement très connue)

Arriverez vous à entendre ce que ces trois triangles veulent vous dire ? Une preuve sans mot proposée par Jérôme Germoni.

4.6.6 Quel est l'âge d'Esteban (el Capitan) ?

Un des plus jolis problèmes sur l'âge du capitaine, qui va nous faire parcourir de l'arithmétique en haute mer ! Mais pas d'inquiétude, le Capitaine Esteban nous amènera à bon port !

4.6.7 007 contre S_{26}

Voici un exercice récréatif qui permettra de réviser nos classiques sur le cours groupes et anneaux (groupe de permutation, anneau $\mathbb{Z}/n\mathbb{Z}$).
Cet exercice est extrait du site les mathematiques. net et a été proposé par GaBuZoMeu
`https://les-mathematiques.net/vanilla/index.php?$p=/discussion/2334798/la-gaffe-de-007`

4.6.8 Ampoules et interrupteurs en caractéristique 2

Une histoire d'ampoules et d'interrupteurs... et de formes quadratique sur le corps $\mathbb{F}_2$!

4.6.9 Popcorn maths 'n burger quizz

Le petit quizz du jour qui se joue avec cinq nombres réels.

4.6.10 Le corbeau et le renard, une fable mathématique

Le corbeau et le renard expliqué à une machine ! Mais les machines ont-elles de l'humour ? Peut-on traduire, « il était une fois », par « il existe » ? et la morale de l'histoire, par un théorème ?
Mickael Launay en est l'auteur (il me l'a signalé après que j'aie posté la vidéo). Merci à lui pour cette fine analyse de texte, cette fidèle traduction et ce bel hommage à Monsieur de la Fontaine.
La prochaine fois, nous verrons le corbeau et le renard en langage inclusif.

4.6.11 Des voeux de bonne année selon une tradition familiale...

... dans les familles de mathématiciens ! Pour une bonne année 2021, on va visiter ce nombre et une propriété particulière qui nous fera passer, pour le plaisir, par les sommes de Cauchy, les formes quadratiques réelles, et même les disques de Gershgorin... Tout un programme !

4.6.12 Equations grégophantiennes-1

Nous allons voir en trois vidéos comment résoudre des équations sur le calendrier grégorien. Par exemple : une année de municipales à Lyon est tombée un dimanche 21 avril. Quelle est cette année ?

4.6.13 Equations grégophantiennes-2

On trouve une formule explicite pour calculer n'importe quel jour de la semaine est associé à une date. Mais les formules ne sont pas encore prêtes pour résoudre des équations « grégophantiennes ».

4.6.14 Equations grégophantiennes-3

On finit par résoudre l'énigme du Dimanche 21 avril. Etonnament, c'est un système de congruence qui va nous y amener.

4.6.15 2021 et le jour de pi-1

La racine carrée de 98723 est 314, 2021..., ce qui en fait un nombre emblématique pour le jour de pi. Mais, au fait, comment trouver tous les entiers dont la racine carrée a ses premières décimales qui commencent par 2021 après la virgule ? Ce petit problème d'approximation diophantienne est le point de départ d'un joli voyage en arithmétique.

4.6.16 2021 et le jour de pi-2

Et nous voici partis dans une histoire de recherche de points entiers entre deux droites. Malheureusement, les pentes de ces droites ont des vecteurs entiers trop grands pour que les choses soient bien visibles. On a alors recours aux fractions continues pour approcher au mieux ces pentes.

4.6.17 2021 et le jour de pi-3

Et la lumière fut ! On utilise le groupe $GL_2(\mathbb{Z})$ pour voir plus finement les choses sans changer la nature entières du problème. On retrouve toutes les solutions avec aisance et un minimum de calcul.

4.6.18 Maths et Pizzas

Nous parcourons ici une brève histoire de la pizza, et sur la façon dont les mathématiciens ont abordé, du XVII-ème siècle à nos jours, les problèmes liés à cette invention majeure de l'humanité.

4.6.19 Concours SMF-Junior 2022-Algèbre

Le concours SMF Junior est probablement le défi le plus haut perché pour nos étudiants en mathématiques. Je propose de faire de la retape ce concours prestigieux dans un premier temps, puis, de corriger le problème qui a été donné en algèbre. On parlera donc du dénombrement des sous-espaces stables par un endomorphisme nilpotent (sur un corps fini).

4.6.20 Pavage d'un ballon de foot par des hexagones ?

Amis footeux bonsoir ! On va montrer qu'il est impossible de paver un ballon par des hexagones. La même étude nous montrera que la chose est possible si le ballon est torique. Et cette possibilité n'est pas qu'une performance sportive, c'est également un moyen raffiné de voir un isomorphisme exceptionnel entre $PSL_2(\mathbb{F}_7)$ et $PGL_3(\mathbb{F}_2)$.

4.6.21 Galois et Hilbert ou les avatars de la dualité

On présente un tableau d'analogies entre trois théories : la dualité des espaces vectoriels, la correspondance de Galois et le théorème des zéros de Hilbert.

4.6.22 La cohomologie sans effort (pour celles et ceux qui savent poser une addition) -1

Inspiré par un exposé de Jérôme Germoni, on présente ici la cohomologie des groupes à l'aide d'une opération que tous nos élèves de 6ème connaissent bien et qui se révèlera par la suite être le générateur d'un second groupe de cohomologie célèbre...

4.6.23 Cohomologie des groupes et suites exactes scindées-2

On définit ici à partir de deux groupes G et K, avec K abélien, et une action de G sur K par automorphismes, le deuxième groupe de cohomologie $H^2\ (G, K)$. On montre comment associer à une extension de G par K, un élément de $H^2\ (G, K)$. On montre comment cet élément permet de voir si K possède un complément dans cette extension.

4.6.24 Cohomologie et théorème de Schur-Zassenhaus-3

Ce troisième volet sur la cohomologie nous montrera comment réduire en poussière le théorème de Schur-Zassenhaus (cas abélien) à l'aide de la cohomologie. On prouvera dans un second temps (mais sans cohomologie) comment le cas général s'en déduit, c'est-à-dire qu'un sous-groupe distingué d'ordre n d'un groupe d'ordre nm, avec n, m premiers entre eux, possède un complément.

4.6.25 Cohomologie par l'exemple- les groupes d'ordre 8- (video-4)

On propose, sans aucune technique particulière, présenter la cohomologie des groupes avec des petits calculs élémentaires et concrets. On construit tous les groupes possédant $\mathbb{Z}/2\mathbb{Z}$ comme sous-groupe distingué avec un quotient isomorphe au groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, c'est-à-dire finalement tous les groupes d'ordre 8 à l'exception du groupe cyclique.

4.6.26 Cohomologie et la bijection extensions-H^2

Après avoir donné quelques exemples qui décrivaient le lien entre extensions et second groupe de cohomologie, il est temps de présenter le résultat phare qui permet de comprendre pourquoi la cohomologie est devenue le graal de la théorie des groupes : la bijection entre classes d'extension d'un groupe G par un groupe abélien A et le groupe de cohomologie $H^2\ (G, A)$.

4.6.27 La caractéristique 2 avec une rampe de spots

Une histoire d'ampoules et d'interrupteurs... et de formes quadratique sur le corps $\mathbb{F}_2$!
On va introduire deux problèmes autour d'ampoules et interrupteurs sous forme de quizz (niveau minimal $L3$ pour le premier et $M1$ pour le second). Dans les deux cas, la solution doit son salut à l'intervention de formes quadratiques sur $\mathbb{F}_2$. Ou plutôt, de formes bilinéaires symétriques sur l'espace $\mathbb{F}_2^n$, ce qui, en caractéristique 2, est assez différent.
On compte ensuite le nombre de solutions au problème des rampes de spots et on se ramène à dénombrer le groupe orthogonal $O_n(\mathbb{F}_2)$, ce qui se fait par récurrence.

4.6.28 La trigonométrie, selon Eisenstein

Dans son article de 1846, Gotthold Eisenstein propose une nouvelle approche plutôt révolutionnaire, de la trigonométrie. Son avantage est d'être calibrée pour une théorie en pleine expansion, celle des fonctions elliptiques. Cette vidéo nous présente le tour de force d'un génie des mathématiques trop tôt disparu.

4.6.29 Variance des inversions, polynômes générateurs et décomposition de Bruhat

Un mélange instructif et passionnant de citation de papillote, de variance sur le groupe symétrique, de petits calculs polynomiaux qui nous amènent curieusement à la décomposition en cellule de la variété de drapeau (mais on le dira un peu autrement, avec des matrices). Feat. Stella (la star !)

4.6.30 La formule du binôme quantique

Voici une formule de combinatoire qui généralise la formule bien connue du binôme de Newton. Mais cette formule, au lieu de s'interpréter avec les parties à m éléments dans un ensemble à n éléments, concerne les sous-espaces de dimension m dans un espace de dimension n sur un corps de cardinal q. On profitera du contexte pour introduire la notion de type d'un sous-espace de K^n et de cellules de Schubert de la grassmannienne.

4.6.31 Le théorème de Bruck-Ryser

Prêts pour un feu d'artifice de toutes les couleurs des maths ? La preuve du théorème de Bruck et Ryser fait feu de tout bois. Elle utilise à la fois des formes quadratiques, des invocations quaternioniques, des théorèmes de deux ou quatre carrés, des équations matricielles sur une matrice d'incidence, un soupçon de réduction... Toutes ces splendeurs au service du plan projectif fini.

Errata. Cherry me fait remarquer que le plan de Fano est faux. Il faudrait remplacer le cercle circonscrit par un cercle inscrit. Shame on me ! :-o

4.6.32 Le principe d'incertitude d'Heisenberg expliqué à mon voisin Nico

Une vidéo pour expliquer l'iconique principe d'incertitude d'Heisenberg avec un minimum de moyens mathématiques. En effet, on utilisera juste la notion de système linéaire, matrice inversible... et la série géométrique.

4.6.33 Une « preuve superbement simple » selon Terence Tao - Le problème de Kakeya discret

Un ensemble de Besicovitch (qui généralise l'ensemble de Kakeya) est une partie de $\mathbb{R}^n$ dans lesquelles toutes les directions sont représentées. Besicovitch a proposé une version sur corps fini de ce type d'ensemble et Zeev Dvir a donné une borne inférieure pour le cardinal d'un tel ensemble. Au menu, polynômes, corps finis, et combinatoire. Mais avant tout, une preuve superbement simple selon le sympathique médaille Fields Terence Tao.

4.6.34 Dessins d'enfants par Alex Moriani - 1

Alex Moriani vient de présenter son mémoire sur les dessins d'enfants, sous la direction de François Labourie. Il s'agit là d'un pan important de la théorie de Grothendieck-Teichmüller qui permet de mieux comprendre le groupe absolu du corps Q. Dans cette première vidéo, Alex nous présente les premières définitions et premiers exemples.

4.6.35 Dessins d'enfants par Alex Moriani - 2

Voici une présentation (sans preuves, mais avec illustration !) des résultats de Belyi et Grothendieck autour des dessins d'enfants.

4.6.36 Un problème de cinéphile !

Petit problème ludique de géométrie dans une salle de cinéma !

4.6.37 Un exercice proposé par Vincent Lafforgue

Alain Genestier m'a communiqué un exercice de Vincent Lafforgue qui a envoyé un corrigé succinct. Nous en faisons ici une traduction bien moins succincte, mais je l'espère compréhensible par nos étudiants de Master. Merci à Loris d'avoir filmé tout ce temps malgré son rhume : -)

4.6.38 Invitation à la combinatoire quantique

Nous allons revenir sur les bases de la combinatoire classique (nombres binomiaux, formulaire de base, pour repartir d'un bon pied sur la combinatoire quantique et en observer les ressemblances et les différences.

4.6.39 Formalisation informatique de preuves par Loris

https ://youtu.be/EC66JLQnT-4
Loris, actuellement en cursus de Master Avancé de mathématiques, travaille cette année sur la réécriture et la formalisation de preuves. Il a eu l'excellente idée de "formaliser" la preuve d'un développement fétiche de son année d'agrégation : le théorème de Gauss-Wantzl

4.6.40 Les octonions par la construction de Cayley-Dickson

On présente une construction commune, due à Dickson, qui, à partir du corps des réels, fournit le corps des complexes, puis, à partir des complexes, au corps non commutatif des quaternions, pour finir avec les octonion. On complète la construction avec une application éclairante !

4.6.41 C'était comment le bac en 67 ?

Une petite perle au bac Paris 1967. Il s'agit de la structure de groupe sur une hyperbole, et, chose étonnante, quelques applications géométriques, (simples, certes, mais tout de même !) de cette structure ! Chaud quand même les questions ! Doit-on y voir une raison aux évènements de l'année qui a suivi :-) ?

4.6.42 Le problème Bac Paris 69

Jean-Claude Andrieux a passé le bac en 1969 et la vidéo à effet Waouh sur la géométrie du demi-plan de Poincaré

4.6.43 Approximation d'un réel et pavage par des triangles hyperboliques

Quelques belles surprises et de l'effet waouh dans cette vidéo où l'on présente la construction d'un pavage par des triangles hyperboliques dans un premier temps, puis comment ce pavage nous fournit la meilleure approximation de nos réels favoris !

5 C'est graphe docteur ? (7)

5.1 Graphes (a minima) pour l'oral de l'agrégation - 1

On propose ici une petite discussion informelle sur les graphes. D'abord, on parlera de définitions, vocabulaire. Ensuite, de ce que les graphes veulent bien modéliser, et des problèmes que les outils développés dans la théorie veulent bien résoudre. Après avoir passé rapidement sur les algorithme, on attaque le lemme des poignées de mains, avec un joli problème... de poignées de mains.

5.2 Graphes (a minima) pour l'oral de l'agrégation - 2

On regarde les longueurs de chemins le long des arêtes d'un graphe, ce qui nous amène naturellement du côté théorique, vers des problème de puissances de matrices, donc de réduction, et du côté de la modélisation, vers des problèmes de type « évolution probabiliste ». Ensuite, on s'intéresse aux graphes sous-jacents de polyèdre. On peut alors, rien qu'avec la structure de graphe, classifier les solides platoniciens, et voir que l'on ne pourra jamais paver un ballon de foot avec des hexagones, ce qui ne nous a pas empêcher de gagner le mondial en 1998...

5.3 Graphes (a minima) pour l'oral de l'agrégation - 3

On termine avec quelques petites choses sur le nombre chromatique et des petites choses afférentes.

5.4 Nombre chromatique d'un graphe et théorème spectral

Le nombre chromatique d'un graphe est le nombre minimal de couleurs que l'on peut attribuer à ses sommets pour que deux sommets connectés soient de couleurs différentes. On prouve une inégalité sur le nombre chromatique d'un graphe en fonction du spectre de sa matrice d'adjacence. L'inspiration provient de la jolie épreuve 1 de l'agrégation interne de 2019.

5.5 Inégalités de Cheeger pour les graphes

L'étude des graphe passe souvent par celle de sa matrice d'adjacence, qui, comme toute matrice réelle symétrique, possède une suite décroissante de valeurs propres réelles. Nous allons voir (découvrir ?) que la robustesse du graphe, c'est-à-dire, sa capacité à rester connexe même si on en retire des sommets, dépend de la position de la seconde valeur propres par rapport à la première.

5.6 Un exercice sur les graphes et la star $\zeta(2)$!

Voici un exercice assez élémentaire sur la coloration des graphes qui fera curieusement intervenir la fonction zeta en 2 et donc le fameux nombre *pi*. Il est inutile de savoir quoi que ce soit sur les graphes pour se retrouver dans un problème de dénombrement qui amène naturellement à la série de Riemann.

5.7 Le théorème de l'amitié

Tout ce qu'on aime dans un problème d'algèbre : un bel habillage avec une histoire d'amitié, de la réduction, des matrices symétriques, de la combinatoire et un peu d'arithmétique ! Elle est pas belle, la vie ?

6 On finit en chanson !

6.1 U-Turn (Philippe) par Guillaume Mallet

Une année belle année de prépa pleine d'émotions, qui finit en chanson, avec Guillaume et sa cover de U-Turn (Lili)

6.2 Tarare (et on a fait des maths)

A joint work of U.C.B.L (United Choir of Baire Lovers) and Topoldavy University

6.3 La dernière échéance, United Choir of Baire Lovers

Une petite vidéo souvenir de ces moments passés à préparer l'agreg externe sous confinement.

6.4 Le banquet final à la Chapelle

Une année pleine d'émotion, d'échanges, d'espoirs, de réussites... ou pas. Mais une année qui se termine en chanson !