Le jardin des plaisirs

Phil Caldero

6,02k abonnés 1250 vidéos

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'')

Tuto du catalogue des vidéos de la chaîne (le jardin des plaisirs) (12'40') "Self-evidence" Tribute for the 60th anniversary of the March on Washington (4'12'')

(757 vidéos dont 216 pour l'externe et 493 rediff. En bleu, l'AI (voire l'AE) et, en rouge, l'AE pure)

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

Table des matières

0 -Un peu de lecture (12)

Carnet de Voyage en Algébrie : la présentation (24’27’’)

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

Carnet de Voyage en Analystan : la présentation (13’51’’)

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

Algèbre éclectique de Danila-Eiden-Mneimné-1 (14’43’’)

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

Algèbre éclectique de Danila-Eiden-Mneimné-2 (12’29’’)

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

Algèbre éclectique de Danila-Eiden-Mneimné-3 (19’08’’)

On étudie **les idéaux premiers** de l'anneau (intègre) $Z[X]/(X^4+1)$. 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, $F_p[X]$**)

Algèbre éclectique de Danila-Eiden-Mneimné-4 (15’16’’)

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** !

"Le groupe symétrique S_4 et ses métamorphoses" 1 (14’25’’)

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.

"Le groupe symétrique S_4 et ses métamorphoses" 2 (17’38’’)

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

"Le groupe symétrique S_4 et ses métamorphoses" 3 (15’25’’)

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.

"Le groupe symétrique S_4 et ses métamorphoses" 4 (16’09’’)

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 3-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**.

"Le groupe symétrique S_4 et ses métamorphoses" 5 (17’47’’)

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).**

Les perles d'Indra par David Mumford (and al.) (1h40’57’’)

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**. 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.

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".

On veut maintenant que **le collier de perles soit constitué de disques tangents entre eux**. Cela demande déjà au départ que les quatre 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 cycliquement tangents alors les points de tangence sont cocycliques.**

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 $x^2+y^2+z^2-xyz=0$.

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- Propédeutique (33)

Cahier de vacances-Théorie des ensembles (25’10’’)
Cahier de vacances-Complexes (23’48’’)
Cahier de vacances-Suites (18’01’’)
Cahier de vacances-Fonctions continues (20’45’’)
Cahier de vacances-Polynômes (38’30’’)
Cahier de vacances-Espaces vectoriels (20’57’’)
Cahier de vacances-Applications linéaires (35’19’’)
Cahier de vacances-Dimension (44’03’’)
Cahier de vacances-Matrices (28’54’’)
Cahier de vacances-Matrices-2 (18’41’’)

Questionnaire sur les ensembles et applications (31’29’’)
Questionnaire sur les structures algébriques (22’50’’)
Questionnaire sur l’arithmétique-1 (30’37’’)
Questionnaire sur l’arithmétique-2 (32’54’’)
Questionnaire sur le groupe de permutations (22’55’’)
Questionnaire sur les polynômes (31’19’’)
Questionnaire sur les espaces vectoriels (26’00’’)
Questionnaire sur les espaces euclidiens-1 (45’40’’)
Questionnaire sur les espaces euclidiens-2 (21’38’’)
Questionnaire sur les matrices (25’43’’)
Questionnaire sur les déterminants (21’57’’)
Questionnaire sur la réduction-1 (30’04’’)
Questionnaire sur la réduction 2 (15’47’’)
Questionnaire sur la réduction-3 (18’44’’)
Questionnaire sur les séries entières (18’21’’)
Questionnaire sur les séries (23’20’’)
Questionnaire sur les suites (25’09’’)
Questionnaire sur la topologie (23’41’’)

Propédeutique. Les nombres complexes (décomplexés) pour l'AI (37’45’’)
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 et géométrie des complexes).

Petit recueil d'idées reçues-1-espaces-vectoriels (11’33’’)
Petit recueil d'idées reçues-2-réduction (14’32’’)
Petit recueil d'idées reçues-3-Polynômes-Groupes-Anneaux (16’41’’)
Petit recueil d'idées reçues-4-formes-quadratiques (10’55’’)

2 - Cours (102)

Cours d'algèbre linéaire

Espaces vectoriels (2h03'50'')

On commence **un cycle d'algèbre linéaire qui figure au cœur du programme d'algèbre de l'agrégation interne**. Ici, il sera question de la définition des espaces vectoriels.
On attaque les premières définitions dans les espaces vectoriels : **parties libres, parties génératrices**.
On découvre le **lemme d'échange qui permet de prouver que toutes les bases d'un espace vectoriel de dimension finie ont même cardinal.**
On montre enfin **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 problèmes sur corps finis.
On a vu que **toute partie libre peut être complétée en une base**. Ce résultat a **son équivalent pour les parties génératrices : on peut en extraire une base. C'est 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).**
En fait, la plupart des espaces vectoriels, que l'on considère, **sont des sous-espaces vectoriels d'espaces de référence**. On traite donc 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**.
On change d'envergure avec **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.
On définit **les deux opérations (addition et intersection) sur l'ensemble des sous-espaces vectoriels d'un espace vectoriel** 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 vectoriels considérés**.
On commence avec des **applications de la formule de Grassmann**. On continue avec **la définition de la somme directe de deux ou plusieurs sous-espaces** et quelques critères de sommes directes.
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).

Applications linéaires (1h18'05'')

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.
Premières définitions autour des applications linéaires : on définit **les applications linéaires entre deux espaces vectoriels**. Après quelques motivations, on en donne une forme générale lorsque les deux espaces sont les K-espaces K^n. On donne un **exemple fondamental d'isomorphisme avec l'application qui, à un vecteur, associe son n-uplet de coordonnées dans une base fixée**.
Opérations sur les applications linéaires : ce volet parle **des objets et théorème fondamentaux autour des applications linéaires : l'addition, la multiplication par un scalaire, la composition et, enfin, le théorème fondamental qui assure l'existence et l'unicité d'une application à partir de l'image de l'espace de départ**.
Théorème fondamental de l'algèbre linéaire : dans cette vidéo, **on traite de l'injectivité et de la surjectivité, qui sont les deux ingrédients de la bijectivité. On commence par faire quelques petits rappels de ces notions dans le cadre de la théorie des ensembles, puis, on regarde comment détecter l'injectivité et la surjectivité dans le cadre de l'algèbre linéaire (en dimension finie)**. On commence par des objets géométriques (noyau et image), puis des entiers (dimensions des noyaux et images) et, enfin, on finit par des critères par l'image d'une base.
Applications injectives et surjectives : it's play time ! On va maintenant tester nos connaissances en matière d'applications linéaires en comptant sur un corps fini tout ce que l'on a défini et étudié.
Dénombrement sur corps fini : on attaque **le théorème central du cours sur les applications linéaires** (qui aura un avatar encore plus puissant avec les matrices !), **la formule du rang qui met en relation la dimension du noyau d'une application linéaire f de E dans F, le rang de f (la dimension de l'image) et la dimension de l'espace de DEPART**. Comme corollaire, **on en déduit une caractérisation de la surjectivité par la dimension du noyau et dans le cas particulier où dim(E)=dim(F) (par exemple pour les endomorphismes), qu'injectif est équivalent à surjectif**. On donne deux contre-exemples en dimension finie.
La formule du rang et ses corollaires : une vidéo de synthèse pour tester notre compréhension du cours et de toutes ces petites choses qui se cachent derrière. **On calcule le nombre d'applications linéaires surjectives d'un espace vectoriel vers un autre (sur un corps fini). L'idée est de basculer, à l'aide de la formule du rang, de la surjectivité, à l'injectivité, que l'on sait faire, puisque l'on sait compter les parties libres.**

Dualité (2h29'07'')

Le dual est à la dualité ce que le conjoint est au couple. C'est dire si l'affaire est sérieuse ! On commence par parler de **ce que l'on appelle le dual** mais, surtout, **la dualité (en dimension finie)**. On exhibe, tout d'abord, **un tableau qui transforme un objet de l'algèbre linéaire en un objet "dual"**. Ensuite, on définit **la "base duale" en dimension finie**, on écrit deux formules qui se révèleront très pratiques, dans la suite, et on fournit **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 dual 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 bi-dual**.
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 bi-dual 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 bi-dual 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**.

Matrices (1h26'34'')

On introduit enfin **les matrices comme objet de calcul au service des applications linéaires**. Pour l'instant, on observe **les liens entre matrices et applications linéaires 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, la transposée et 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 **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** puis on montre que **cette définition permet de retrouver très facilement toutes les formules sur les matrices de passage**.
On discute et on prouve enfin **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**.

Déterminant (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 $M_n(K)$ dans 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.**

Réduction polynômes d'endomorphisme 1 (13'34'') 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.
Réduction polynômes d'endomorphisme 2 (14'22'') On commence par **définir les polynômes d'un endomorphisme u d'un espace vectoriel E**. Ceci est défini comme **un morphisme d'algèbre allant de l'algèbre de polynômes 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**.
Réduction polynômes d'endomorphisme 3 (15'24'') 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"**.
Réduction polynômes d'endomorphisme 4 (12'36'') 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**.
Réduction polynômes d'endomorphisme 5 (10'38'') On prouve ici **le théorème de Cayley-Hamilton par les matrices compagnon**.

Réduction polynômes d'endomorphisme 6 (15'48'') Les propriétés du polynôme caractéristique : degré, indépendance du corps, divisibilité par le polynôme minimal mu et divise μ^n.

Réduction polynômes d'endomorphisme 7 (17'25'') 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.

Les polynômes (1h33'52'')

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. Dans un premier temps, il s'agit de premières définitions et d'arithmétique des polynômes à travers l'évaluation et la division euclidienne : on définit ici l'anneau des polynômes A[X] (ou K[X]) sur un anneau intègre unitaire A (ou sur un corps K) et on en donne une "base", on étudie la notion de degré et ses propriétés qui permettent de définir une division euclidienne. On traite de l'injection naturelle de A dans A[X] et, enfin, cette spécificité de l'anneau de polynôme : le morphisme d'évaluation. A partir de là tout s'enchaîne : l'anneau K[X] est principal donc factoriel. On étudie, ensuite, les anneaux quotient de K[X] par un idéal (forcément principal) et on montre que si P est non nul K[X]/(P) est un K-espace de dimension deg(P).

On en vient à des aspects plus éloignés de l'arithmétique comme les racines d'un polynôme, les polynômes versus les fonctions polynômes. On fera également un détour du côté du résultant et on finira par les relations coefficients/racines...

On introduit le problème : comment trouver des racines d'un polynôme de A[X]. Cette vidéo est juste un balbutiement sur la nature arithmétique de la recherche de racine : un polynôme qui possède une racine fixée a est forcément multiple de (X-a). Lorsque P annule plusieurs racines distincts a_i, alors P est multiple du produit des ($X-a_i$). On étudie la K-algèbre des fonctions polynômes en prenant soin de la distinguer de la K-algèbre des polynômes. Cette distinction se fait à l'aide d'un morphisme d'algèbres entre les deux (de la seconde vers la première). Si le corps K est infini alors le morphisme est un isomorphisme et on peut confondre les deux algèbres. On fait l'étude lorsque le corps K est fini où l'on exhibe le noyau du morphisme.

On introduit un outil majeur pour comprendre le PGCD de deux polynômes P et Q : le résultant. Pour cela, on introduit le résultant comme le déterminant de la matrice d'une application linéaire qui est isomorphe si et seulement si P et Q sont premiers entre eux. L'avantage d'avoir un tel critère de primalité entre P et Q par un déterminant est de pouvoir décliner le résultat dans des extensions mais, surtout, dans des quotients si P et Q sont à coefficient dans un anneau. On fait également des petits calculs de discriminants en degré 2 et 3.

On commence ici à s'intéresser aux relations coefficients/racines en introduisant de façon naturelle la notion de polynôme symétrique élémentaire et on énonce, sans le prouver, pour de sombres raisons d'hygiène corporelle, le théorème fondamental de polynômes symétriques qui annonce que tout polynôme symétrique de $Z[X_1, ..., X_n]$ s'écrit de façon unique comme polynôme à coefficient entier des polynômes symétriques élémentaires. On illustre ce théorème sur un exemple avec la somme s_2 de Newton avant d'attaquer les identités de Newton qui fournissent la somme de Newton s_k par récurrence en fonction des polynômes symétriques élémentaires à n variables. Tout d'abord pour k=n à l'aide de la matrice compagnon, puis pour k plus petit que n et k plus grand que n à l'aide de deux astuces classiques. Pour finir, on résout un "système symétrique" à trois variables.

Réduction diagonalisation 1 (17'48'') 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.

Réduction diagonalisation 2 (10'53'') 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 et 3) diagonalisabilité des endomorphismes de multiplication par une matrice.

Réduction diagonalisation 3 (15'09'') On tente ici de définir des fonctions "inverses" sur les matrices, comme la racine kième, le logarithme... On se rend compte que même si ces fonctions existent bien sur C, elles ne sont pas forcément définissables sur $M_n(C)$. 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 astucieusement les séries de Taylor par des polynômes en une matrice nilpotente.

Réduction trigonalisation 1 (12'53'') 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.

Réduction trigonalisation 2 (15'48'') 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".

Réduction trigonalisation 3 (19'15'') 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 de 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.

Réduction et formes normales (16'05'') 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 et, 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.

Réduction et invariants de similitude 1 (16'50'') On a collecté suffisamment de résultats généraux pour commencer 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...

Réduction et invariants de similitude 2 (18'27'') 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 (1h06'12'')

On va commencer une petite série sur les équations matricielles vues 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 K et X une matrice de $M_n(K)$. 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 simples, 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 R. Les méthodes précédentes nous ont permis de résoudre le problème dans C mais comment obtenir les solutions sur R ? Le résultat repose sur **une propriété essentielle de la réduction : deux matrices réelles C-semblables sont R-semblables. On a le même résultat en remplaçant (R, C) par (K, L) où L est une extension de K**.

On montre ici quelques techniques (non exhaustives) pour trouver les racines kièmes 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**. Errata : lire$(1+x)^{1/k}$ au lieu de $(1+x)^{1/n}$ dans la vidéo puis mettre l'égalité à la puissance k.

Enfin, **on revient sur ce petit lemme qui permet de passer d'un développement de Taylor, sur 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 kièmes, logarithmes).

Topologie en algèbre linéaire (1h33'29'')

On commence un nouveau volet sur la topologie des espaces vectoriels réels et complexes, en dimension finie, et liée à la réduction. Pour débuter d'un bon pied, on parle du **théorème d'équivalence des normes : deux normes définissent la même topologie**. Ou, dit autrement, toute boule ouverte pour une norme contient une boule ouverte pour l'autre norme (et inversement). Donc, en théorie, on pourra parler de topologie normique sans préciser le choix de la norme. Et en pratique, selon le type de problème posé, on pourra choisir la norme qui nous convient le mieux.

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 : critères de convergence de suites géométriques de matrices, méthodes de Newton pour la résolution d'équations, définition de fonctions analytiques, preuves de propriétés de type algébrique par restriction à une partie dense, caractérisation topologique de propriétés liées à la réduction. On donne aussi des contre-exemples au théorème d'équivalence des normes (corps non complet, dimension infinie).

Après avoir défini la topologie ambiante, on commence les premières avancées dans l'outil topologique pour la réduction. On commence tout d'abord avec **le théorème fondamental qui dit qu'en dimension finie toute forme linéaire est continue** et ses conséquences. Ce théorème va nous permettre d'étudier un par un **les invariants utilisés dans la réduction sous l'angle aigu de la continuité. Le déterminant, la trace, le polynôme caractéristique, fournissent des fonctions continues**. En revanche, le rang est semi-continu, inférieurement, ainsi que le polynôme minimal (pour la relation divise).

On attaque l'étude générale de la suite géométrique (A^m) où A est une matrice carrée complexe. On tombe comme on pouvait s'y attendre à une condition sur le spectre, avec une condition particulière pour la valeur propre 1. On finit par un florilège d'applications, d'exemples d'utilisation sur l'association topologie et réduction (on renvoie l'internaute aux livres **Carnet de Voyage en Analystan** et **Carnet de Voyage en Algébrie** pour des énoncés et des preuves précises) allant des suites géométriques de matrices, suites linéaires récurrentes d'ordre k, suites homographiques, théorème de Perron-Frobenius, application de la densité de GL_n, des matrices diagonalisables à valeurs propres distinctes sur C.

Formes quadratiques-1 (1h22'02'')

Les formes quadratiques exposées pour un cours d'agrégation interne (et externe si on généralise à un corps de caractéristique différente de 2). On trouve dans ce premier cours **toutes les premières définitions et toutes les connexions entre formes quadratiques, formes bilinéaires symétriques, matrices symétriques et changement de base**.

Dans cette deuxième partie, on attaque (enfin !) **des exemples classiques : formes quadratiques sur les espaces R^n, sur les espaces de polynômes et enfin sur les espaces de matrices**.

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.

Formes quadratiques-2 (1h37'57'')

Nous cherchons, maintenant, **les formes quadratiques telles que tout sous-espace possède un orthogonal en somme directe. Sur 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, avec les motivations qui s'imposent, **la notion d'adjoint d'un endomorphisme**.

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, enfin, **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**.

Le principe du min-max (44'51'')

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 (BON). On va donner une caractérisation de ses valeurs propres à l'aide de la forme quadratique que S définit naturellement sur R^n par q(x) = (x, Sx). C'est **le principe du min-max appelé, également, théorème de Rayleigh**.

Partie II. On vient de voir une version préliminaire du principe du minimax. 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 en prouvant les inégalités de Weyl et le théorème d'entrelacement de Cauchy.

Prépa à l'écrit - Formes quadratiques 1/8 (15'55'') 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 $OA^2+OB^2+OC^2=3OI^2+2/3\ AJ^2+1/2\ BC^2$ (au lieu de $OA^2+OB^2+OC^2=4/3OI^2+2/3\ AJ^2+1/2\ BC^2$)
Prépa à l'écrit Formes quadratiques 2/8 (17'22'') 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 à l'écrit Formes quadratiques 3/8 (16'18'') 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 complétait en une base orthonormée. Là, c'est pareil, sauf qu'il n'y a pas de base orthonormée.
Prépa à l'écrit Formes quadratiques 4/8 (14'01'') On présente progressivement le principe de Rayleigh ou principe du mini-max en petite dimension. Il s'agit d'une caractérisation géométrique des valeurs propres. On en donne une application amusante sur une fonction trigonométrique.
Prépa à l'écrit Formes quadratiques 5/8 (16'40'') 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 à l'écrit Formes quadratiques 6/8 (15'18'') 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 à l'écrit Formes quadratiques 7/8 (15'33'') 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 à l'écrit Formes quadratiques 8/8 (16'34'') 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 $M_2(Z)$ sont Z-semblables en leur associant des formes quadratiques. La Z-similitude s'interprète alors sous forme de congruence des formes quadratiques.

Questionnaire sur les formes quadratiques (1h 08'14'')

**

Matrices hermitiennes 1 (18'13'') Voici un premier volet sur les formes hermitiennes. On suppose connus les résultats analogues sur les formes bilinéaires symétriques (congruence, Sylvester et théorème spectral) et on donne le résultat équivalent dans le cas hermitien.
Matrices hermitiennes 2 (20'48'') 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, le fait 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 (BON) si et seulement s'il commute avec son adjoint.
Matrices hermitiennes 3 (18'14'') On donne des exemples célèbres de matrices normales : matrices hermitiennes, anti-hermitiennes, unitaires et leurs équivalents réels. On fait ensuite le point sur la façon dont les matrices hermitiennes et anti-hermitiennes généralisent la partie réelle et imaginaire...

Géométrie affine- le minimum vital à l'interne (43'08'') Un beamer pour présenter le minimum à savoir sur la géométrie affine aux écrits de l'agrégation. Au menu : structure affine (version 1 et 2), sous-espaces affines, applications affines, repères affines et représentations matricielles, recherche de point fixe et un petit formulaire de survie.
Géométrie affine 1 (16'40'') 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.
Géométrie affine 2 (13'55'') 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, à un bipoint, associe un vecteur puis une définition des transformations affines. Mais, on lui préférera la définition par les actions simplement transitives d'un espace vectoriel. Dans ce cadre, les notations et, surtout, la définition des transformations affines, sont plus naturelles.
Géométrie affine 3 (13'08'') 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 ϕ de l'espace. Or, l'existence d'un point invariant est liée à la réduction (1 est-il dans le spectre de ϕ ?). Nous voilà revenu dans notre domaine de connaissance!
Géométrie affine 4 (18'13'') 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 o phi o b^{-1}, et donc, finalement, on peut assimiler f et ϕ, ce qui est bien agréable. Malheureusement, on va devoir étudier les isométries qui ont 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 o et sa représentation matricielle en affine.

Géométrie affine 5 (19’08’’) On prouve le théorème principal de ce cours : le théorème de décomposition réduite qui donne une condition générale pour qu'une application affine se décompose de façon 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.

Géométrie affine euclidienne 1 (10’46’’) 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 leurs endomorphismes associés, c'est-à-dire les isométries vectorielles, vérifient la propriété demandée pour obtenir la décomposition réduite.
Géométrie affine euclidienne 2 (8’32’’) 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.
Géométrie affine euclidienne 3 (13’49’’) On attaque la classification en dimension 3. Au programme, symétries glissées et vissages qu'il est bon de connaître. Un rapide coup d'œil à la dimension n nous convaincra que la classification n'est pas beaucoup plus difficile !
Géométrie affine, barycentres et convexité 1 (12’02’’) 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 (homogénéité, 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 cœur de la notion d'espace affine (réel).
Géométrie affine, barycentres et convexité 2 (10’35’’) 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.

**

Sous-espaces stables 1 (20’31’’) 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.
Sous-espaces stables 2 (20’18’’) On attaque les problèmes de sous-espaces stables en lien avec le polynôme caractéristique. Celui-ci est irréductible sur 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.
Sous-espaces stables 3 (10’11’’) 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 autoadjoints, normaux, diagonalisables et, pour finir, lemme de Fitting et sous-espaces caractéristiques.
Sous-espaces stables 4 (10’39’’) 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.
Sous-espaces stables 5 (20’40’’) 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.
Sous-espaces stables 6 (10’17’’) On finit en donnant quelques indications sur la façon de décrire tous les sous-espaces stables d'un endomorphisme.

Le résultant (46’01’’) On introduit, définit et obtient une expression du résultant, en insistant sur l'application linéaire dont il est issu plutôt que sur l'expression du déterminant qui le définit habituellement. On se propose de donner rapidement un panel d'exemples de calculs du résultant et 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 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 algébriques et résultant (cas des coniques), de courbes algébriques (cas plus général), équations cartésiennes d'une courbe rationnelle... et on finit avec une surprise : Résultant et Jacobien

Cours arithmétique

Premier cours d'arithmétique (2h02'50'')

On fait ici **le point sur les équations sur l'anneau Z des entiers : linéaires, affines, à plusieurs inconnues, quadratiques et, enfin, polynomiales sur le corps Q**.

On introduit l'arithmétique. Vu l'abstraction de ce qui viendra par la suite, il est i**mportant de faire un préambule qui permettra de se fixer les idées et d'avoir à sa disposition un vivier d'exemples**. On commence donc un premier volet introductif, où on montre **des techniques de résolution d'équations diophantiennes (i.e. dans l'anneau des entiers). Ici, il sera question d'équations linéaires sur Z, où le lemme de Gauss joue un rôle décisif.**

On résout ici 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 donnaient pas un aperçu suffisamment général de la situation.

On traite 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**.

On attaque le cours d'arithmétique avec **l'étude de l'anneau Z**. On suit **une procédure que l'on retrouvera avec d'autres anneaux, comme par exemple l'anneau des polynômes 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.

On décrit **l'ensemble des idéaux de 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 Z et les entiers naturels (car 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**.

On présente 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, çà et là, **le lemme de Gauss et, son avatar, le lemme d'Euclide**.

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.

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.

Fonctions arithmétiques à l'agrégation (43'00'') 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 ϕ d'Euler et la fonction μ de Moebius**. On continue avec **l'ubiquité de la fonction μ 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 ζ**.

Prépa à l'écrit Arithmétique 1 (17'32'') On résout ici l'équation diophantienne $x^2+y^2-29z^2=0$ en mettant l'accent sur **la factorialité de l'anneau Z[i] des entiers de Gauss**.

Prépa Ecrit Arithmétique 2 (9'39'') 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 Z[i] des entiers de Gauss**.

Prépa à l'écrit Arithmétique 3 (17'59'') 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 α(p) divise n... Et nous voici embarqués dans de curieuses considérations, à 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 à l'écrit Arithmétique 4 (11'58'') On présente, dans Arithmétique 4 et 5, deux exercices qui ont pour but de **présenter l'utilisation classique du lemme chinois**. Le premier exercice consiste à calculer le nombre d'endomorphismes polynomiaux inversibles en un endomorphisme fixé, sur un corps fini. **Le lemme chinois est ici dans sa version polynomiale**. La notion d'anneau local est sous-jacente.

Prépa à l'écrit Arithmétique 5 (11'12'') 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 Z/mZ.

Prépa à l'écrit Arithmétique 6 (16'56'') 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 α(m) divise n.

Prépa à l'écrit Arithmétique 7 (4'44'') 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 α(m) divise n. Pour connaître α(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 $p\geq3$ et p=2.

Prépa à l'écrit Arithmétique 8-teaser (4'09'') 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 à l'écrit Arithmétique 8 (17'25'') 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 Z. On montre que cet ensemble est soit trivial, soit isomorphe à Z.

Prépa à l'écrit Arithmétique 9 (16'45'') 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 à l'écrit Arithmétique 10 (18'20'') 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 à l'écrit Arithmétique 11 (16'38'') 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 à l'écrit Arithmétique 12 (16'26'') 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 $P(0)\neq 0$. Errata : la borne du nombre de racines est m^s et non pas ms comme annoncé !

Structures quotients (1h25'58'')

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 domaines (ensembles, groupes, espaces vectoriels, réduction, anneaux, équations diophantiennes). Le quotient d'un ensemble par une relation : on montre qu'une application est une bijection qui s'ignore, on présente le quotient d'un groupe par un sous-groupe non nécessairement distingué puis on montre comment obtenir des structures de groupes quotient à l'aide d'un sous-groupe distingué. Dans un deuxième temps, on s'attaque maintenant aux structures d'espace vectoriels quotient. On en trouve des bases, on déduit la dimension de l'espace quotient et on remarque que la formule du rang est totalement naturelle dans ce contexte. Ensuite, une preuve élégante (mais classique !) de l'essoufflement de la suite des noyaux emboîtés est présentée. Elle utilise le passage au quotient. Enfin, on se dirige maintenant vers l'arithmétique en introduisant les idéaux qui permettent de construire des structures d'anneaux quotient, tout en généralisant la relation "divise" des entiers. On en profite pour montrer comment les structures quotient peuvent amener à résoudre des équations diophantiennes.

Prépa à l'écrit. Gymnastique des corps 1 (13'37'') Dans la série de vidéos qui suit, il ne s'agira pas de théorie des corps, 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.

Prépa à l'écrit. Gymnastique des corps 2 (10'07'') Après avoir étudié les spécificités des corps infinis ou finis, on s'attaque au cas des corps de caractéristique zéro ou p.

Prépa à l'écrit. Gymnastique des corps 3 (14'22'') 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).

Prépa à l'écrit. Gymnastique des corps 4 (15'54'') 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 informations 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.

Prépa à l'écrit. Gymnastique des corps 5 (16'09'') 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.

Prépa à l'écrit. Gymnastique des corps 6 (12'45'') On pénètre ici le cœur du problème : montrer que deux matrices carrées sur un corps K sont semblables si et seulement si elles sont semblables sur une extension L. Cette preuve se fait en deux temps : un premier temps où 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.

Prépa à l'écrit. Gymnastique des corps 7 (7'26'') 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.

Les réseaux aux écrits de l'agrégation (1h04'52'')

On aborde ici une étude de réseaux dans 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 Z (sous-groupe de 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 Z^n, en suivant en filigrane l'épreuve EP1 de l'agrégation interne 2012. On prouve l'existence de Z-bases, après avoir prouvé l'unicité du cardinal de telles bases. On prouve ensuite que ces bases sont en bijection avec le groupe $GL_n(Z)$. 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 Z^n en prouvant l'existence d'un Z-base pour tout sous-groupe G de Z^n et même une condition pour qu'un élément du sous-groupe G se complète en une Z-base de G. On va faire quelques prolongations avec une adaptation sur 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 mains) avec le théorème de la base adaptée.

Cours groupes

Les groupes cycliques (1h08’03’’)

On introduit **les groupes cycliques**, d'une manière un peu grossière (comme **groupe isomorphie à Z/nZ**) puis, de manière plus abstraite (**groupe fini monogène**). On donne ensuite quelques exemples (et contre-exemples) de groupes cycliques dans la nature.

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 Z/nZ 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.

On déduit ainsi 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 (Z/pZ*, x). On montre ensuite le rapport avec les 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.

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

Introduction aux actions de groupes par le dénombrement (1h30’05’’)

Une petite introduction qui j'espère, vous convaincra de **l'utilité très concrète des actions de groupes**. Au 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**.

Lemme du berger et axiomatisation : on va montrer dans cette vidéo **comment les groupes permettent de compter**. Ici, on dévoile **la stratégie des groupes** : une machine de guerre pour **créer des situations où le lemme du berger peut s'appliquer**.

Groupe symétrique et action naturelle : on attaque, tout de suite, avec l'exemple du groupe symétrique. On voit **comment les nombres multinomiaux découlent de la formule des classes (sauf qu'il n'y a qu'une seule classe)**.

Groupe linéaire et action naturelle : on passe facilement du groupe symétrique au groupe linéaire en remplaçant sous-ensemble par sous-espace et partitions par sous-espaces en somme directe. On obtient des dénombrements où les factoriels sont remplacés par des cardinaux de groupes linéaires sur un corps fini.

Dénombrer les matrices diagonalisables : on s'attaque au **nombre de matrices diagonalisables sur un corps fini** en obtenant une jolie formule.

Les séries génératrices dans le dénombrement : **la jolie formule obtenue** pour dénombrer les matrices diagonalisables est peu utile en l'état. Elle **comporte trop de termes quand le corps devient grand**. Toutefois, on peut la réarranger car **plusieurs termes sont regroupables**. On peut alors donner **une estimation de la probabilité de choisir une matrice diagonalisable au hasard sur un corps fini**. On finit sur ce résultat épatant.

On dénombre les matrices de rang r : on souhaite **compter le nombre de matrices de taille (m, n) de rang r sur un corps fini de cardinal q**. On utilise ici **les actions de groupes**. Pour l'instant, on se contente d'un calcul préliminaire : celui du calcul du nombre de sous-espaces de dimension k fixée puis on s'attaque au nombre de matrices de taille (m, n) et de rang r sur un corps fini. On en profite pour **présenter l'action de Steinitz qui partitionne l'espace des matrices selon leur rang**. Une fois le nombre de matrices de rang r obtenu, on lui donne une forme plus parlante, pour y découvrir des phénomènes naturels comme **l'isomorphisme canonique et la dualité**. On peut retrouver cet exercice dans **Nouvelles Histoires Hédonistes de Groupes et de Géométries I-3.6**.

Questionnaire Groupes : Action (ou vérité) (58’19)

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. Nous allons parler d’actions du groupe symétrique, du groupe cyclique, de GL_n sur K^n, de Steinitz, de GL_n sur des espaces de matrices et enfin diverses actions (O_n, espaces affines...).

***

Mini-cours de théorie des représentations 1 (15’51’’) 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.

Mini-cours de théorie des représentations 2 (8’18) 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 Z/3Z qui nous permet de comprendre ce qui se passe, pour tout groupe cyclique, puis le premier groupe non abélien S_3.**

Mini-cours de théorie des représentations 3 (13’37’’) On définit les représentations, les morphismes de représentations, et on montre le théorème de Maschke.

Mini-cours de théorie des représentations 4 (15’16’’) On s'attaque à **la classification des représentations d'un groupe**. Par Maschke, on voit qu'il suffit de trouver toutes les représentations irréductibles. Ces dernières se trouvent **toutes dans la représentation dite régulière du groupe**, qui est un cas particulier de représentation par permutation.

Mini-cours de théorie des représentations 5 (11’52’’) On prouve ici le théorème d'orthonormalité des caractères avant d'en découvrir les multiples corollaires.

Mini-cours de théorie des représentations 6 (16’32’’) On donne ici l**es 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**.

Mini-cours de théorie des représentations 7 (10’11’’) 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.

Mini-cours de théorie des représentations 8 (11’22’’) 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 ?**

Mini-cours de théorie des représentations 9 (14’30’’) 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.**

Mini-cours de théorie des représentations 10 (16’48’’) **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.**

Mini-cours de théorie des représentations 11 (14'30'') 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**.

Mini-cours de théorie des représentations 12 (15'19'') 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 et, d'autre part, comme groupe d'isométries positives du cube.

Mini-cours de théorie des représentations 13 (14'24'') 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.

Mini-cours de théorie des représentations 14 (13'29'') 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.

Mini-cours de théorie des représentations 15 (9'48'') On prépare une petite extension du lemme de Schur dans le cas où la représentation 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 (non moins élégante !).

Mini-cours de théorie des représentations 16 (14'47'') 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**.

Mini-cours de théorie des représentations 17 (17'09'') 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**.

Mini-cours de théorie des représentations 18 (16'21'') 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 pouvoir retrouver tous les sous-groupes distingués de G**. On regardera, dans la prochaine vidéo, **des sous-groupes distingués particuliers comme le centre et le groupe dérivé**.

Mini-cours de théorie des représentations 19 (23'59'') On montre, de façon pratique et de façon théorique, puis sur des exemples, **comment obtenir le centre et le groupe dérivé de la table de caractères**.

3 – Algèbre linéaire (79)

Les délices de matrices (63)

1 - Matrices d'applications linéaires

Critère par les mineurs pour le rang d'une matrice (20'46'')

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, R ou C, à la topologie du rang (Nouvelles histoires hédonistes chapitre I).

Sous-espaces de matrices avec des conditions de rang-1 (8'26'')

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 (20'39'') 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

Matrices compagnon, preuves et applications (16'39'')

On introduit et on donne un aperçu (avec preuves) de **la propriété fondamentale des matrices compagnon d'un polynôme unitaire P : son polynôme minimal et son polynôme caractéristique sont égaux à P**. On fournit ensuite pêle-mêle (sans preuves mais avec références) bon nombre d'applications. On finit enfin avec un petit exercice (corrigé) qui pourrait en étonner plus d'un.

Exercices Réduction (15'42'')

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.

Critère de nilpotence par la trace et application (13'21'')

Voici une preuve express du **critère de nilpotence par la trace** que l'on peut trouver dans **Carnet de Voyage en Algébrie**. Tellement express qu'on peut se permettre d'y ajouter une application, courte, mais élégante.

Petit exercice ludique sur les matrices entières inversibles (4'33'')

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

Un scoop sur Cayley-Hamilton ? (17'50'')

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) (14'20'')

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" (15'11'')

Deux exercices (plus une variante) où **l'arithmétique des polynômes vient délivrer la réduction de ses problèmes de diagonalisabilité** !

Décomposition de Dunford pour de "petits" polynômes minimaux (27'11'')

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 (21'23'')

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 (26'51'')

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** et 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 multivariable".

Endomorphismes de l'espace des matrices qui commutent à la transposée (21'15'')

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 à 3 méthodes : résolution par la dualité, les matrices diagonalisables ou les matrices trigonalisables.**

Un exercice classique sur le commutant (20'25'')

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 (cas algébriquement clos puis cas quelconque), une preuve topologique et une qui provient de la combinatoire algébrique (tableaux de Young).**

Tout sur le commutant (1ère partie) (11’56’’)

On propose de **faire le point de 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) (21’28’’)

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 (22’57’’)

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 ! (15’45’’)

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 Q est 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 ? (10’10’’)

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

Sous-espaces de matrices stables par conjugaison (18’41’’)

On va trouver **tous les sous-espaces de $M_n(K)$ stables par conjugaison de $GL_n(K)$**. 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 (18’15’’)

On discute ici de **résultats sur les sous-espaces de $M_n(K)$ constitués de matrices toutes diagonalisables**.

Un exercice sur les suites récurrentes linéaires et barycentres (18’17’’)

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 barycentres**. On donne ici **deux versions de l'exercice et deux solutions, une élémentaire et l'autre niveau M1**.

Comatrice, qui es-tu ? (6’14’’)

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) (11’48’’)

On s'intéresse à la question I 6) 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'ordre : 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) (13’39’’)

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 n b) dont le noyau est de dimension 1 c) d'indice 3 en dimension 6.

Le corps C est algébriquement clos (preuve par la réduction) (16’17’’)

On propose **cette preuve du théorème de d'Alembert-Gauss (C est algébriquement clos)**, adapté d'une preuve de Pierre Samuel **dans le cadre de la réduction des endomorphismes**. On peut trouver cette preuve dans Carnet de Voyage en Algébrie I-3.37.

Utilisation de la réduction en géométrie affine- un exemple (29’07’’)

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**.

Un exercice sur autour du théorème spectral (formule d'Apollonius) (15’46’’)

La formule d'Apollonius relie les distances entre les sommets d'un triangle et le milieu d'un côté. Le théorème spectral permet d'en voir une généralisation tous azimuts en dimension n.

Semblables sur C vs semblables sur R (13’32’’)

Deux matrices réelles sont semblables sur C si et seulement si elles sont semblables sur 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**.

3 – Systèmes linéaires

Pseudo-inverse d'une matrice réelle (27’06’’)

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 (23’15’’)

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 (15'38'')

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 (20'37'')

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

4 – Matrices et norme euclidienne

Le théorème spectral (et ses avatars) (31'08'')

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 Algèbre.

Introduction aux matrices de Gram (16'50'')

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 (10'12'')

On montre ici que **le rang de la matrice de Gram d'une famille de vecteurs de 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 dégénérescence d'une forme bilinéaire symétrique par restriction**.

Gram-Schmidt et la décomposition QR (25'22'')

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 (16'17'')

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 C sont $GL_n(C)$-semblables si et seulement si elles sont $O_n(C)$-semblables. On utilisera une "pseudo-décomposition polaire" sur C, que nous démontrerons dans une prochaine vidéo.

MG-2023-Partie IV-pseudo décomposition polaire sur un corps (28'37'')

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.

Décomposition polaire-Appellation controlée-1 (31'15'')

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 $O_n(C)$. Attention, contrairement à ce que l'on pourrait penser, il ne s'agit pas d'un nième 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 (24'48'')

Après avoir vu la décomposition polaire de divers sous-groupes de $GL_n(R)$ ou $GL_n(C)$, 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 (50'22'')

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 $GL_n(R)$. 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 (12'02'')

On propose ici de regarder la décomposition polaire sous un angle géométrique. On donne une preuve géométrique de l'existence et une interprétation géométrique de l'unicité de la décomposition orthogonale et d'une matrice symétrique.

Une nouvelle preuve du théorème spectral ? (15'05'')

Une preuve nouvelle, 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 (11'07'')

Une jolie proposition de Hugues Contini pour une preuve du théorème spectral : 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) (8'09'')

Voici une preuve très stylée du théorème spectral, proposée par Toto-toto. Il s'agit d'une preuve totalement algébrique (modulo C est algébriquement clos qui finalement n'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 ! (18'54'')

Une preuve originale 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 (34'34'')

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 relations peuvent être proches et même très proches…

5 – Matrices et topologie

Critère topologique de diagonalisabilité (21'58'')

Sur C, une matrice est diagonalisable si et seulement si sa classe de similitude est fermée pour la topologie d'espace normé de $M_n(C)$. On montre ce résultat ainsi que son analogue sur R.

L'intérieur des matrices diagonalisables complexes (14'20'')

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 https://studio.youtube.com/video/dQs-...

Continuité du spectre d'une matrice (22'59'')

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.

Matrices borderline (à l'agrégation):

Prépa AE : Matrices échelonnées 1 (17'16'')

Les matrices échelonnées 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 dans la géométrie de la Grassmannienne**. On va essayer de vous faire aimer cette théorie en dévoilant, 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 AE : Matrices échelonnées 2 (10'47'')

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 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 AE : Matrices échelonnées 3 (13'29'')

On attaque **maintenant l'injectivité** et, pour cela, on veut retrouver, de façon intrinsèque, **une matrice échelonnée à partir d'un sous-espace de 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 AE : Matrices échelonnées 4 (17'43'')

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 (42'34'')

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 numérique matricielle et à l'optimisation.

La dualité dans le théorème de Frobenius (24'19'') **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 (31'49'')

L'ensemble des matrices nilpotentes de $M_n(C)$ 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 (15'57'')

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 $GL_n(Z)$**.

Décomposition LU- un survol rapide des choses à bien connaître (11'41'')

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)

Trigonalisation- l'exercice coup de cœur (7'57'')

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 $GL_n(F_p)$, 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 $GL_n(F_p)$ et, enfin, théorèmes de Sylow !**

Lemme de Brauer sur les matrices de permutation (38’25’’)
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 $GL_n(K)$, c'est-à-dire semblables**. 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 $GL_n(K)$**. Dans un premier temps, **nous supposons que le corps 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 K est de caractéristique quelconque** et une jolie matrice symétrique réelle va nous tirer d'affaire.

Déterminant droit devant (6)

Un calcul de déterminant (sans les mains) (13’41’’)
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" (12’39’’)
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.

Un (non-)calcul de déterminant (13’42’’)
On se propose de **calculer le déterminant de la représentation réelle d'une matrice complexe**. Selon comment on attaque ce détermina nt, **le calcul peut devenir inextricable... ou simple comme bonjour**.
Volume de la n-boule et intégrale de Wallis (18’31’’)
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 π et, pour n=3, le célèbre 4/3 π. Et quelle est sa limite quand n tend vers l'infini ?
Irréductibilité du déterminant (good proof/bad proof) (19’36’’)
On va montrer de deux manières que **le déterminant, vu comme polynôme à n² indéterminées, est irréductible**. Une première preuve, élémentaire, 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**.

Formule de Binet-Cauchy (par la face sud) (20’27’’)
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.

Corps finis à l’envi (7)

Les classes de similitude en dimension 2 (sur corps fini) (23’52’’) **Rien de mieux pour comprendre les classes de similitude que de les décrire en totalité** dans l'espace des matrices $M_2(K)$ **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 (18’26’’) 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 Mn(K) tend vers 1/n! dans K est grand.**
Sous-espace de matrice diagonalisables sur F_p (8’48’’) On cherche **un contre-exemple de sous-espace de matrices toutes diagonalisables sur un corps fini, sans la condition de diagonalisabilité.**
Nombre de matrices nilpotentes sur un corps fini (22’53’’) **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. (26’34’’) On va attaquer un problème un peu ardu qui ne demande que des choses solubles dans l'agrégation. On va montrer que **la probabilité de choisir une matrice semi-simple dans $M_n(K)$ avec K fini, tend vers 1 quand le cardinal de K tend vers l'infini**. Le plus long finalement dans la preuve est de faire un inventaire des prérequis. 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 (14’36’’) 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.
Questions autour de l'automorphisme de Frobenius (16’55’’) **L'automorphisme de Frobenius possède bien des aspects : c'est un morphisme de corps, un endomorphisme d'espace et 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.
Corps finis. Construction par les corps de rupture. (17’36’’) On construit généralement le corps fini F_q comme corps de décomposition du polynôme X^q-X. Voici une construction qui part de rien (ou presque) et construit le corps F_q comme corps de rupture d'un polynôme irréductible de degré n sur F_p, avec $q=p^n$.

4 - Les groupes sous tous les angles (34)

1 – Groupes finis

Critère de cyclicité pour les groupes finis (16'13)

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 et qu'il a 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 (10'53'')

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} (15'45'')

Nous venons de voir dans une vidéo précédente que **les classes de conjugaison de S_n sont 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 (10'05'')

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} (21'07'')

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 (15'30'')

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**... Vous pouvez trouver une belle application avec un jeu de cartes sur Des cartes bien à...

Le collier de perles ou le coloriage du n-gone (59'42'')

Voici **une présentation** (un peu improvisée) **du collier de perles en trois parties plus un épilogue. Il s'agit de problèmes de dénombrement par action d'un groupe cyclique**. On répond à une question très naturelle des **coloriages du n-gone modulo isométrie et non plus modulo rotation**. Ceci nous même à observer **le groupe diédral**, on finit sur une formule générale du nombre de coloriages qui distingue le cas pair et le cas impair.

Sous-groupes d'indice 2 d'un groupe fini (15'13'')

Voici un petit exercice sur **l'existence d'un sous-groupe d'indice 2 dans un groupe fini d'ordre 2n, n impair**. Une **application remarquable du théorème de Cayley**. Remarque pertinente de Rached Mneimné : parmi les groupes finis d'ordre pair qui ne possèdent pas de sous-groupes d'indice 2, j'ai parlé de groupes simples non abéliens mais j'ai omis de mentionner le groupe A_4, d'ordre 12 qui ne possède pas de sous-groupe d'ordre 6. On peut s'en convaincre en disant qu'**un sous-groupe d'indice 2 est distingué, donc union de classes de conjugaison, ce qui est impossible pour A_4 au vu du cardinal (1,3,8) de ses classes de conjugaison**.

La formule de Dobinski (finie) (21'39'')

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 (9'55'')

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.

2 – Sous-groupes de GL_n - groupe orthogonal

Le groupe orthogonal (engendrement en toute simplicité) (1h09'08'')

Un grand classique ! On étudie **le groupe orthogonal d'un espace euclidien**. On s'intéresse, dans un premier temps, à **l'engendrement du groupe orthogonal par des réflexions orthogonales** puis, on montre le résultat classique de **l'engendrement du groupe spécial orthogonal par des retournements orthogonaux**. Puis, on attaque ici **la simplicité de SO_3**. Il ne faudra pas moins de deux vidéos pour en venir à bout.

Tout (ou presque) sur le groupe orthogonal ! (31'16'')

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

Sous-groupes compacts de $GL_n(R)$ (21'42'')

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 $GL_n(R)$.** Dans un deuxième temps, on passer à un théorème plus difficile mais fondamental : **tout sous-groupe compact est conjugué à un sous-groupe de 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 $GL_n(C)$ (22'25'')

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

3 – Groupes en analyse

Sur le groupe des homéomorphismes de R (22’52’’) Quelques aspects "groupistes" de l'ensemble des homéomorphismes de R, muni de la loi o. **On s'intéresse ici à un objet essentiellement analytique avec un regard d'algébriste**.

Groupes en action borderline :

Un théorème de Jordan sur le groupe linéaire modulo n (21’40’’) Un **petit théorème de Jordan qui nous emmènera sur les rivages du groupe linéaire $GL_k(Z/nZ)$ et qui vient généraliser l'indicatrice d'Euler (pour k=1).** On pourra **voir dans ce théorème une extension du domaine du lemme chinois !**

Le groupe dérivé :

Tout sur le groupe dérivé- 1/2 (14’02’’) **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 (13’41’’) Dans cette seconde partie, on calcule encore deux **sous-groupes dérivés : celui du groupe alterné A_4 et du groupe spécial linéaire $SL_2(F_3)$**. On attaque **des applications : l'utilisation du groupe dérivé dans les groupes simples d'ordre 60, l'étude des morphismes de $GL_n(K)$ 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 (22’42’’) **Pour les oraux d'agrégation externe, si l'on a montré lors d'un développement que tel (SO_3) 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) ? (24’42’’)
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** !

Sous-groupes finis de $GL_2(R)$ et $GL_2(Z)$ (25’20’’) Voici dans le cadre de l'agrégation externe, **un petit théorème sur la classification des sous-groupes finis de GL2(R) et GL2(Z)**.

Morphismes entre groupes abéliens finis (la Saga des GAF) (27'56’’) 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 et mise en forme matricielle.
Morphismes entre groupes abéliens finis-2 (Le bureau des GAF en gros) (22’10’’) Voici le 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 Z/2ZxZ/4Z et de Z/2ZxZ/6Z ?** 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 (45’38’’) 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 (14’30 ’’) 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 animé de grands mathématiciens, de Galois, dans sa lettre testamentaire, jusqu'aux grands mathématiciens du XXème 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 (15’53’’) On attaque ici **le cas des isomorphismes dits exceptionnels pour les corps F_4 et F_5**. On conseille, pour ceux qui seraient intéressés de les comprendre tous (!), la lecture du chapitre XII de H2G2 (2015)

Construire un automorphisme extérieur de S_6 (15’19’’) **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 (6’21’’) Cette vidéo est une présentation des vidéos qui vont suivre. On y explique **un schéma général 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 points 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 (17'49'') On attaque donc un critère permettant de **voir si la table de caractère d'un groupe fini est à valeurs dans Z**. On passe par un petit lemme sur les extensions 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 (14'56'') On commence **notre traque du nombre d'or ϕ**. 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 ω est une racine primitive 5-ième 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 (20'42'') 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 (30'59'')

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 (38'22'')

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 (38'21'')

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 de la théorie des représentations mais son but non avoué est de participer à cette familiarité !

5– Arithmétique, anneaux, corps et polynômes (49)

Arithmétique (19)

Deux équations diophantiennes quadratiques (17’34’’)

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

Le problème des diviseurs de Dirichlet (11'27’’) et Le problème des diviseurs de Dirichlet-2 (13’37’’)

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 fonds abyssaux. Voici un petit exposé du problème 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 (31’53’’)

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 nombres 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 (20’11’’)

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 (13’14’’)

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 (29’04’’)

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[5]. Même si on pourra trouver des méthodes 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 (37’38’’)

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

Un exercice qui utilise le lemme chinois (23’56’’)

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 p premiers à 120 et $p \equiv 3[4]$?

Exercices Arithmétique 1 (10’09’’)

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...

Exercices Arithmétique 2 (15‘46’’)

On résout des petites 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 Arithmétique 3 (12‘37’’)

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 Arithmétique 4 (9’54’’)

On résout un petit système de congruence dans un cadre "hors lemme chinois" avant de le modéliser sous forme de suite exacte de groupes.

Loi complémentaire de réciprocité quadratique au bac ! (7’35’’)

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)^{p²-1)/8}.

La fonction totient de Jordan (16’01’’) On introduit cette fonction de l'arithmétique, due à Jordan, qui généralise l'indicatrice d'Euler en "dimension k". On utilisera, comme c'est souvent le cas avec les fonctions arithmétiques, la convolution de Dirichlet ainsi que la fonction de Moebius.

Codage RSA, décodage et cryptanalyse (29’00’’)

Comme application classique du lemme chinois, on présente ici le codage RSA, son décodage, avec un exemple. Moins classique, nous allons présenter 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 Z/nZ.

Système RSA-1 Codage et décodage (17’10’’)

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 : ϕ (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 (16’03’’)

Cette seconde vidéo traite de l'attaque dite, de Fermat, et d'une autre forme d'attaque, plus empirique.

Système RSA-3 Attaque de Wiener (15’15’’)

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 $x^d \equiv x^n$ [n] mais c'est $(x^e)^d \equiv x$ [n].

Anneaux (4)

Entiers de Gauss, factorialité, et cercle rationnel-1 (18'35'')

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 π**. On montre que **ce sont juste les 4 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 (7'24'')

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 π 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) (31'12'')

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

X^p -a et l'alternative irréductible/existence de racine (9'31'')

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

Corps (2)

Introduction au corps gauche des quaternions- (X-ENS-2023) -1 (20'23'')

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".**

Introduction au corps gauche des quaternions- (X- ENS-2023) -2 (22'33'')

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** !

Polynômes (8)

Un exercice sur le thème "polynôme, racines et multiplicités" (10'13'')

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 importante 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.

Un exercice qui utilise des polynômes (6'02'')

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

Exercice sur polynômes et PGCD (AE 2021 Spécial docteur) (9'51'')

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** !

Décomposition des polynômes cyclotomiques modulo p (26'41'')

On donne ici **une description de la décomposition en irréductibles du nième 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 cœur) (14'41'')

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 Z. On utilise ici les discriminant du polynôme X^{n-1} ainsi que l'anneau des entiers algébriques.

Polynômes cyclotomiques (petits calculs entre amis) -1 (16'30'')

On introduit **les polynômes cyclotomiques et les deux formules qui permettent de les définir**. Une formule qui les définit, 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 soit 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.

Polynômes cyclotomiques (petits calculs entre amis) -2 (21'15'')

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

Polynômes cyclotomiques (petits calculs entre amis) -3 (19'59'')

On termine ce petit exposé sur **le calcul des polynômes cyclotomiques avec le calcul des polynômes Φ_{pq}, premiers**. On va voir **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=3x5x7=105. On finit sur un exemple en calculant Φ_{60}.

**

Arithmétique mon cœur à reclasser (7)

Coprimalité, Moebius et Zeta par Arthur (24'58'') Arthur et sa craie Excalibur viennent nous présenter un **développement transversal sur les thèmes du dénombrement, de l'arithmétique et des 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 : à 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 différent de 1.
Les menteurs de Miller-Rabin- test de primalité (25'53'') 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 est-on sûr que n est premier si tous les nombres choisis ont passé le test ? Y a-t-il des menteurs ?

Les nombres pseudo-premiers de Perrin-1 (15'08'') 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.
Les nombres pseudo-premiers de Perrin-2 (12'53'') On achève la preuve du fait que **p premier implique que le pième 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.**
Les nombres pseudo-premiers de Perrin-3 (17'57'') 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**.
Les nombres pseudo-premiers de Perrin-4 (11'23'') 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**.

Arithmétique borderline pour l'agrégation :

Exercices Réseaux (15'49'') On a souvent besoin en arithmétique d'utiliser de choses élémentaires sur les réseaux. **A l'écrit, la caractérisation des Z-bases de Z^n et un "théorème de la 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.

Carrés en tout genre (9)

Loi complémentaire de réciprocité quadratique (un exercice du cours de D. Perrin) (7'15'') Une preuve très simple pour montrer que **2 est un carré modulo p (impair) si et seulement si p ≡ 1 ou -1[8]**.

Le théorème des deux carrés par l'approximation rationnelle (13'50'') Voici **une preuve élémentaire du théorème des deux carrés qui utilise un théorème d'approximation rationnelle que l'on prouve (également de façon élémentaire) dans les suites de Farey**.
Les suites de Farey 1/2 (25'56'') et les suites de Farey 2/2 (11'32'') Mathématiques récréatives aujourd'hui ! Avec les suites de Farey si simples à définir mais si profondes en conjectures, si simples à définir 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 (24'58'') 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 (17'34'') Une suggestion de notre follower "Pastix51" 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 (16'10'') A la suite d'une conversation avec Pastix51, 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(x²_1+x²_2+x²_3+x²_4) ² et on aurait 2p²=(x²_1+x²_2+x²_3+x²_4) ², ce qui est absurde car 2 n'est pas un carré...

Fonctions qui préservent les sommes de carrés par Jamil-1 (16'44'') 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 (12'54'') On finit ce joli exercice avec la preuve du lemme. Pythagoriciens, pythagoriciennes, bonsoir !

6- Les formes quadratiques en éveil (19)

Qui es-tu, forme polaire ? (22’35’’)
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 à digérer un cours sur les formes quadratiques**.

Formes de Hankel 1/7 (4’46’’) et Formes de Hankel 2/7 (6’53’’) 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.
Formes de Hankel 3/7 (2’13’’) Une troisième vidéo pour trouver **la matrice de la forme de Hankel**.
Formes de Hankel 4/7 (7’20’’) 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 $\boldsymbol{\alpha_i}$ ne sont plus forcément ni distincts ni réels mais s'ils ne sont pas réels, ils seront conjugués. **On voyage des relations coefficients/racines, en passant par le théorème de Sylvester et on parvient au signe du discriminant**.
Formes de Hankel 5/7 (4’30’’) On va ici enfin (il était temps !) **définir la forme de Hankel associée à un polynôme réel en toute généralité**.
Formes de Hankel 6/7 (7’13’’) On veut dans cette vidéo calculer **la signature de la forme de Hankel associée à un polynôme réel** T.
Formes de Hankel 7/7 (5’57’’) On prouve **le théorème de Hankel : la signature de la forme de Hankel d'un polynôme réel T "voit" son nombre de racines réelles et son nombre de racines distinctes**.

Les formes de Hankel (à leur état naturel) (13’42’’) **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 R**.
Les formes de Hankel au naturel-2 (11’12’’) **Nous présentons maintenant le cas général**.

Représentation d'entiers par une forme quadratique-somme de carrés-1 (15’29’’) 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 et d=1,2,3,5. Nous allons voir que le cas d=5 diffère des trois premier cas.
Représentation d'entiers par une forme quadratique-congruences-2 (9’03’’) 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 congruences de p**. Nous montrons l'implication (facile) dans un premier temps.
Représentation d'entiers par une forme quadratique-factorialité-3 (19’34’’) 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 !
Représentation d'entiers par une forme quadratique-classes de congruences-4 (18’59’’) 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 Z^2.**
Représentation d'entiers par une forme quadratique-5 (17’13’’) On a vu dans la vidéo précédente que **la réciproque qui consiste à partir de p premier $\equiv$1 ou 9 [20] implique que p est représenté par x^2+5y^2 demande une connaissance sérieuse des classes de congruences de formes quadratiques sur 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 !
Représentation d'entiers par une forme quadratique-la trilogie-6 (49’39’’) 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...

Forme quadratique sur l'espace des matrices carrées (18’24’’) Un petit exercice autour d'**une forme quadratique intrigante sur l'espace $M_n(K)$.** 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 R).

Formes quadratiques sur le corps des rationnels par Adem Zeghib (28’34’’) 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**.

Tout tétraèdre est régulier (en toute dimension) ! (25’09’’)
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.

7- Bouquet de géométries (45)

Le cercle des neuf points par le calcul complexe (et en neuf minutes !) (12'53'') 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.

Quadrilatères et réduction des endomorphismes (23'17'') Plusieurs thèmes en fusion dans ce petit exercice de géométrie faisant référence au théorème de Thébault (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.

Les tutos géométriques du Père Castor : Géométrie affine euclidienne (10'22'') 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.
Les tutos géométriques du Père Castor : Puissance d'un point, axe radical (14'02'') 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.
Les tutos géométriques du Père Castor : Droites tangentes à deux cercles données (7'52'') 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.

Les coniques. Un exercice képlerien (qui plaira !) (20'26'') 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.

Un exercice sur les coordonnées barycentriques d'un triangle (15'16'') 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 l'objet image que l'on va rencontrer...

Le groupe des isométries du tétraèdre agit sur ses sommets (25'47'') 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.

Composée d'isométries planes-1 (21'34'') Un petit compte-rendu sur la composée d'isométries planes.
Composée d'isométries planes-2 (7'46'') 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.

Exercices Homographies (16'45'') 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.

Ellipse de Steiner 1/6 (15'53'') 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.
Ellipse de Steiner 2/6 (11'03'') 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.
Ellipse de Steiner 3/6 (10'39'') 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 suffisant pour démarrer.
Ellipse de Steiner 4/6 (9'25'') 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.
Ellipse de Steiner 5/6 (10'48'') On est en mesure de calculer l'équation de l'ellipse sous une forme dont on sait déduire les foyers.
Ellipse de Steiner 6/6 (9'08'') 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.

Droites et cercles 1/5 (13'27'') 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.
Droites et cercles 2/5 (9'20'') On présente le groupe des homographies, 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 !
Droites et cercles 3/5 (21'40'') 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.
Droites et cercles 4/5 (13'39'') Dans cette vidéo, on montre que le groupe des homographies agit de façon transitive sur l'ensemble des "cercles et droites".

Droites et cercles 5/5 (5'26'') 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**.

**

Géométrie borderline à l'agrégation :

Cercles tangents (14'20'') 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 (15'14'') 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 anti-homographies) sur les "droites ou cercles"** ainsi que la théorie d'intersection, qui sera à peine évoquée.

Alternative de Steiner (Cercles tangents-3) (6'44'') On présente, sous forme d'exercice corrigé, l'alternative de Steiner. Encore une fois, **les groupes de transformations et leurs invariants** jouent un rôle central.

Alternative de Steiner (Cercles tangents-4) (16'06'') 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 anallagmatique-1 (16'57'') 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 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 anallagmatique-2 (11'55'') On a donné, dans une première vidéo, un tableau qui mettait en **relation des cercles du plan euclidien et des droites de l'espace 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 anallagmatique-3 (18'52'') On commence à minutieusement mettre en place une **correspondance entre droites et cercles du plan complexe, d'une part, et droites de l'espace R^4**. On peut, par section hyperplane, voir tout cela assez agréablement dans R^3 euclidien muni de sa boule unité.

Géométrie des cercles (ou droites) -Pour débuter avec la géométrie anallagmatique-4 (15'29'') Par **cette correspondance que nous avons construite en transformant un cercle en une "droite de l'espace de Lorentz 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 anallagmatique-5 (15'49'') 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 R^4.**

Géométrie des cercles (ou droites) -Pour débuter avec la géométrie anallagmatique-6 (12'03'') On introduit **l'action de $SL_2(C)$ 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 anallagmatique**.

Géométrie des cercles (ou droites) -Pour débuter avec la géométrie anallagmatique-7 (21'15'') On prouve **un isomorphisme entre les groupes simples $PSL_2(C)$ 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 (19'11'') 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 (17'38'') On propose maintenant d'**interpréter les densités d'empilements de sphères**. En dimension 1 (une évidence), en dimension 2 (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 hexagone 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 $GL_3(Z)$-congruentes.

Empilement de sphères 3 (22'10'') 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 (5'37'') 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 connues 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 (15'39'') 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 groupes 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 (10'28'') 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 (11'34'') 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 (11'46'') 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 (10'44'') On a montré le théorème de structure de groupe sur une conique, à l'aide d'un mélange de petits 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 (14'04'') 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 8/9 (5'44) 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.

Structure de groupe sur une conique 9/9 (17'13'') 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.

8 - Un epsilon d'analyse… (26)

Exercices Normes sur R[X]-1 (10'14'')

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

Exercices Normes sur R[X]-2 (9'32'')

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

Exercices Normes sur R[X]-3 (12'14'')

On attaque un petit dernier sur les normes de R[X]. On introduit une norme un peu farfelue sur R[X] et on montre que l'espace 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 R ne peut pas être complet pour aucune norme**.

Normes, boules et stricte convexité 1 (19'34'')

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**.

Normes, boules et stricte convexité 2 (13'43'')

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.**

Normes, boules et stricte convexité 3 (10'05'')

On peut maintenant **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^-.**

Equivalents pour les suites récurrentes (+exemple pour la fonction sinus) (32'38'')

On présente ici **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.**

Comportement asymptotique des suites récurrentes (32'38'')

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, Combinatoire et placements de table (12'55'')), qu'u_n est équivalent à $\sqrt{3/n}$ en l'infini. On cherche ensuite un second terme à son développement asymptotique.

Exercice coup de cœur sur une suite récurrente linéaire (31'50'')

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 cœur 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 !**

Le cercle d'incertitude d'une série entière (18'59'')

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).

Vitesse de convergence d'une suite récurrente (et méthode d'Archimède) (22'17'')

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 $\boldsymbol{\pi}$… et comme on n'est jamais à court d'histoires, on parlera du jeune Grothendieck.

Erreurs dans les calculs d'intégrales-1 (16'19'')

Nous allons parler des **différentes méthodes pour les calculs d'intégrales (rectangle, trapèze, méthode de Simpson).** On commence par une approche algébrique des différentes méthodes connues.

Erreurs dans les calculs d'intégrales-2 (16'02'')

Nous parlons ici de **l'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].

Erreur dans l'approximation par la méthode de quadrature (20'30'') **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 (Méthode de quadrature de Gauss par Caroline (22'25'')), on donnera une estimation de l'erreur commise par cette approche. On finira par une application pour une approximation du nombre $\boldsymbol{\pi}$.

L'intégrale de Dirichlet par Riri (28'06'')

Haut les cœurs ! Riri l'intrépide nous présente **un développement sur l'intégrale de Dirichlet avec une méthode simple et élégante**. Attention, **petite coquille à la fin repérée par @Totototo8119. Il faut lire intégrale de 0 à l'infini au lieu de l'intégrale de 0 à pi/2**. Toujours dans les remarques de **@Totototo8119, 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 l'histoire telle qu'elle s'est déroulée va dans le sens inverse du développement :-)

Nombres de Bernoulli-1 (19'04'') 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.

Nombres de Bernoulli-2 (12'00'') 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!

Nombres de Bernoulli-3 (12'04'') 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.

Nombres de Bernoulli-4 (17'05'') Mais pourquoi les nombres de Bernoulli apparaissent-ils 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.

Nombres de Bernoulli-5 (11'40'') On fait un résumé succinct de l'utilité des nombres de Jacques Bernoulli en analyse (développements limités, trigonométrie, formule de Stirling, approximations d'une intégrale, précision dans la méthode des rectangles) …

Nombres de Bernoulli-6 (22'27'') On prouve une formule qui fournit le dénominateur de tous les nombres de Bernoulli. C'est le théorème de de Clausen-Von Staudt.

Un exercice sur Taylor-Lagrange (13'25'')

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.

Utilisation des fractions rationnelles (dérivées de l'arc tangente) (15'26'')

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...

Problème de la corde universelle (problème d'Olympiades) (18'39'')

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 théorèmes de la corde universelle et l'autre partie nous amènera à un contre-exemple, bougrement tordu, mais sacrément intelligent.

Pourquoi une fonction injective continue sur un intervalle est-elle strictement monotone ? (12'24'')

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

Primitivable implique continue (ou bien) ? (18'32'')

On sait depuis longtemps qu'une fonction continue sur un intervalle 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.

9- Probabilité et combinatoire (8)

Séries génératrices-mode d'emploi (21’24’’) 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 !"

Combinatoire sur le groupe des permutations (18’20’’) Deux petits exercices (en attendant d'en avoir deux plus gros) sur **la moyenne du nombre d'inversions dans le groupe symétrique et la moyenne du nombre de cycles (dans la décomposition en cycles à supports disjoints)**. Référence **H2G2- tome 2 (2015) Chapitre IV**.

Dés pipés et factorisation de polynômes (23’27’’) **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...

Dénombrement et polynômes (dés non pipés) (19’23’’) 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 ! 😉

Borel-Cantelli et les amis de la poésie ! (14’00’’) 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.

L'urne de Polya (tirage avec renforcement) (25’08’’) 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’épilogue, je voulais dire que les X_i suivent une loi de Bernoulli mais leur somme S_n ne suit pas une loi binomiale**.

Tirage de nombres premiers entre eux (33’31’’) **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 ζ débarque dans la théorie des nombres.**

Tirage sans remise de n boules paires (9’53’’) 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 $X_i = 1$**.

Ecrits (73)

Epreuve 1-5 (la partie II)
Epreuve 1-4 (la partie I)
Epreuve 1-3 (l'exercice préliminaire)
Epreuve 1-2 (le vrai-faux)
Epreuve 1-1

2021 :
Epreuve 1-6 : les corollaires du théorème de Burnside
Epreuve 1-5 : Quelques exemples sur Q
Epreuve 1-4 : Quelques exemples
Epreuve 1-3 : théorème de densité de Jacobson (ou Burnside)
Epreuve 1-2 : stabilité et semi-simplicité
Epreuve 1-1 : Préliminaires et palabres

2020 :
Epreuve EP1-2
Epreuve EP1-1

2019 :
Polynômes d'Hermite-EP2-3
Polynômes d'Hermite-EP2-2
Polynômes d'Hermite-EP2-1
Polynômes d'Hermite-EP2

2018 :
Epreuve 1-4
Epreuve 1-3
Epreuve 1-2
Epreuve 1-1

2017 :
Exercices sur les homographies-EP1

2014 :
EP1-parties-I-II

2008 :
EP1-Partie II (30'54'')
EP1-Partie I (37'27'')

Leçons (67)

Leçon 133 AI/101 AE- Groupe opérant sur un ensemble- Applications (55'03'')

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 qui 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**. 00:00 Le 6 minutes 10:32 Questions de jury 30:24 Développements-présentation 30:47 Action fidèle et injection dans un groupe de permutations 40:57 Actions de groupes et dénombrements 50:31 Autres développements

Leçon 133 AI - Groupe opérant sur un ensemble

Leçon-133 AI - Groupe opérant sur un ensemble-Développement-Coloriage du tétraèdre

Leçon 105 AE (102 AI) - Groupe de permutations d'un ensemble fini et applications - 6 minutes et plan

Leçon 105 AE (102 AI) - Groupe de permutations d'un ensemble fini et applications - Développements.

Leçon 105 AE (102 AI) - Groupe de permutations d'un ensemble fini et applications - Questions de jury et exercices

Leçon 106 AI Idéaux d'un anneau commutatif (42'57'')

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 Bézout**. Ensuite, on déroule, **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 système de congruence, et même aux intersections de courbes planes**.

Leçon 107 AE - Représentations linéaires d'un groupe fini 1

Leçon 107 AE - Représentations linéaires d'un groupe fini 2

Leçon 107 AE - Représentations linéaires d'un groupe fini 3

Leçon 113 AE/ 152 AI - Déterminant et applications (47'25'')

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 NH2G2 et dans Carnet de Voyage en Algébrie.

0:00 Présentation et le 6 minutes 8:45 Le savoir-faire autour du déterminant 31:37 Développements proposés.

Leçon 122 AE - Anneaux principaux et applications- la présentation 1

Leçon 122 AE- Anneaux principaux et applications 2

Leçon 122 AE- Anneaux principaux et applications- Evaluation 3

Leçon 122 AE- Anneaux principaux et applications- Harmonisation 4

Leçon 122 AE- Anneaux principaux et applications- Exercices-5

Leçon 122 AE- Anneaux principaux et applications- Exercices-6

Leçon 123 AE - Corps finis et applications

Leçon 125 AE - Extension de corps-exemples et applications 1

Leçon 125 AE - Extension de corps-exemples et applications 2

Leçon 125 AE - Extension de corps-exemples et applications 3

Leçon 125 AE - Extension de corps-exemples et applications 4

Leçon 126-AE - Exemples d'équations en arithmétique 1

Leçon 126-AE - Exemples d'équations en arithmétique 2

Leçon 126-AE - Exemples d'équations en arithmétique 3

Leçon 126-AE - Exemples d'équations en arithmétique 4

Leçon 126-AE - Exemples d'équations en arithmétique 5

Leçon 126-AE - Exemples d'équations en arithmétique-questions de jury 6

Leçon 126-AE - Exemples d'équations en arithmétique-questions de jury 7

Leçon 142 AE (107 AI) - PGCD et PPCM. Algorithmes et Applications 1

Leçon 142 AE (107 AI) - PGCD et PPCM. Algorithmes et Applications 2

Leçon 142 AE (107 AI) - PGCD et PPCM. Algorithmes et Applications 3

Leçon 142 AE (107 AI) - Le contenu de Gauss 4

Leçon 142 AE (107 AI) - La formule pgcd (a, b).ppcm (a, b) = ab dans tous ses états 5

Leçon 142 AE (107 AI) - Tout sur l'algorithme d'Euclide 6

Leçon 142 AE (107 AI) - Invariants du groupe symétrique-PGCD 7

Leçon 144 AE - Racines d'un polynôme fonctions symétriques élémentaires 1

Leçon 144 AE - Racines d'un polynôme fonctions symétriques élémentaires 2

Leçon 144 AE - Racines d'un polynôme-Questions de jury

Leçon 148 AE (110 AI) - La dimension et le rang - 1

Leçon 148 AE (110 AI) - La dimension et le rang - 2

Leçon 148 AE (110 AI) - La dimension et le rang - 3

Leçon 148 AE (110 AI) - La dimension et le rang - 4 Jury
Leçon 149 AE – I - Généralités
Leçon 149 AE – II - Localisation des valeurs propres
Leçon 149 AE – III - Valeurs propres, vecteurs propres. Calculs exacts ou approchés d'éléments propres-Applications
Leçon 149 AE - Valeurs propres, vecteurs propres. Calculs exacts ou approchés d'éléments propres.
Leçon 150 AE - Actions de groupes sur les espaces de matrices
Leçon 159 AE - Formes linéaires, dualité. Exemples et applications
Leçon 159 AE - Formes linéaires, dualité. Exemples et application. Développements.
Leçon 161 AE - Distances et isométries d'un espace affine euclidien 1
Leçon 161 AE - Distances et isométries d'un espace affine euclidien 2
Leçon 171 AE - Formes quadratiques réelles, coniques, exemples et applications
Leçon 190 AE - Méthodes combinatoires et dénombrement
Leçon 190 AE - Questions de jury sur le dénombrement
Leçon 191 AE - Exemples d'utilisation de techniques d'algèbre en géométrie 1
Leçon 191 AE - Exemples d'utilisation de techniques d'algèbre en géométrie 2
Leçon 191 AE - Exemples d'utilisation de techniques d'algèbre en géométrie 3
Leçon 191 AE - Exemples d'utilisation de techniques d'algèbre en géométrie 4
Leçon 191 AE - Exemples d'utilisation de techniques d'algèbre en géométrie 5
Leçon 191 AE - Exemples d'utilisation de techniques d'algèbre en géométrie 6
Leçon 307 AI - Exercices avec utilisation de polynômes irréductibles 1
Leçon 307 AI - Exercices avec utilisation de polynômes irréductibles 2
Leçon 307 AI - Exercices avec utilisation de polynômes irréductibles 3
Leçon 307 AI - Exercices avec utilisation de polynômes irréductibles 4
Leçon 327 AI - Exercices faisant intervenir des automorphismes orthogonaux 1
Leçon 327 AI - Exercices faisant intervenir des automorphismes orthogonaux 2

Développements (62)

ENS '86 Matrices de Moore (feat. Théorème spectral... et la trace) (29’59’’)

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.

Le test de primalité de Lucas-Lehmer (23’49’’)

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**.

Le critère d'Eisenstein (et applications) par Marie (26’35’’)

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 :-)

Le théorème de décomposition de Frobenius par Loïc (25’42’’)

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.

Lemme de Zolotarev- 2 est-il un carré modulo p ? (18’09’’)

Le lemme de Zolotarev crée un lien entre le symbole de Legendre de a [p] et la signature de la multiplication par a. Voici une brèche entre arithmétique et groupes de permutation !

Théorème de progression arithmétique de Dirichlet (version faible) (18’29’’)

Pour tout entier n>0, on montre qu'il existe un nombre fini de nombres premiers congrus à 1 modulo n. On suit une preuve que l'on peut trouver dans Carnet de Voyage en Algébrie.

Les nombres de Bell par Séverine (22’30’’)

Séverine nous présente une formule donnant le nième 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 ζ sur les entiers naturels pairs par Caroline (15‘15’’)

La fonction ζ associe à s>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.

Méthode de quadrature de Gauss par Caroline (22’25’’)

Voir Carnet de Voyage en Analystan (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 !

SO (3) est simple, par Benjamin (32’19’’)

Voici une méthode topologique (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 $SO_2(F_p)$ par Clément (20’24’’)

Clément nous présente un groupe orthogonal fini : le groupe des matrices orthogonales sur le corps fini 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 !

Sous-groupes de R. L'alternative dense/monogène par Caroline (33’19’’)

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...

Nombre de solutions d'une équation dans un groupe fini et table de caractères (18’38’’)

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-Questions du Jury (10’26’’)

C’est le moment des questions pour Luca.

Résoudre un système de congruence par Caroline (16’14’’)

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".

Homéomorphisme de décomposition polaire (11'38'') 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.
La décomposition polaire (par Dom) (25'18'') Dom nous propose le développement classique sur la décomposition polaire. Il s'en suit une série de questions impitoyables du jury.
Volumes et décomposition polaire (24'20'') 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).

Preuve analytique de Cayley-Hamilton par Patrick Sam Al Habobi (26'04'') 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 (18'19'') 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 une jolie formule de résidus matriciels qui permet de définir, en général, l'analogue matriciel d'une fonction (analytique) complexe.

Critère de diagonalisabilité de Klarès par Florence (31'52'') Un joli critère dans un format de développement pour montrer qu'une matrice sur 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 (17'55'') 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.

La suite de polygones par Caroline (14'08'') Caroline nous présente le développement sur la suite de polygones du plan complexe (Carnet de Voyage en Algébrie, 1.3.28). Au programme : réduction, convexité, barycentres, et limites de suites de matrices. Qui dit mieux ?

Condition de cocyclicité de quatre points par Caroline (13'29'') Voici un critère de cocyclicité de quatre points A, B, C et D : l'existence d'un quadruplet de réels non tous nuls a, b, c et d tels que pour tout point M, $aAM^2+bBM^2+cCM^2+dDM^2=0$.

Ellipsoïde de John-Loewner (20'05'') 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 (18'57'') 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 (24'40'') 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.
Fonction Gamma, premières propriétés par Caroline (14'38'') Caroline présente ici les propriétés de base de la fonction Gamma sous un format de développement. On peut trouver la source dans Carnet de Voyage en Analystan.

Noyau de Fejér par Florence (22'40'') 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.

Le théorème de Kronecker (18'19'') 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.

Forme trace et dualité (10'55'') 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 $M_n(K)$.

Théorème de Sophie Germain par Julien (20'34'') 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 !

Théorème de Gauss-Lucas et application par Séverine (15'57'') Un développement tiré de Carnet de Voyage en Algébrie (deuxième 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 (16'59'') 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- Questions du Jury (15'59'') La séance de questions de jury ! Séance qui pourra en éclairer quelques-uns sur la convexité.

Méthode des puissances par Patrick Sam Al Habobi (35'37'') 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 $x_n= Sy_n$.

Le collier de perle (version Kétrane) (38’37’’) 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.

La série harmonique (32’15’’) 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 (18’22’’) 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 (9’58’’) C’est parti pour les questions…
Le théorème de Korovkin et son application au théorème de Weierstrass (30’32’’) 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.

Méthode de quasi-Newton par Patrick Sam Al Habobi-1 (17’34’’) 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 (28’33’’) On aborde ici la séance de questions sur le développement.

L'équation différentielle X'=AX 1/2 (11’56’’) 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.
L'équation différentielle X'=AX 2/2 (12’10’’) On donne une autre approche pour l'allure des courbes dans 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 solutions du système d'équations différentielles X'=AX dans le plan réel par Aurélien (19’31’’) 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.

Le groupe du tétraèdre par Rozenn (18’42’’) Le développement sur le groupe du tétraèdre !

Méthode de Newton pour la décomposition polaire par Antoine 1 (15’24’’) 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.
Méthode de Newton pour la décomposition polaire par Antoine 2 (7’44’’) Le jury (Nicolas et Philippe) pose ses questions à Antoine autour de son développement sur la méthode de Newton.

Le théorème de Bohr-Mollerup par Audrey (22’44’’) 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 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 !

Le théorème de Riesz par Raphaël 1 (12’25’’) 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.
Le théorème de Riesz par Raphaël 2 (7’22’’) Voici le moment des questions du jury. Cela donne une bonne idée de comment les choses se passent le jour J.

La décomposition LU par Patrick Sam Al Habobi (30’32’’) Patrick Sam nous présente la décomposition d'une matrice en une matrice triangulaire inférieure unipotente "L" et une matrice triangulaire supérieure "U", suivi par les fameuses questions du Jury…

Action de Steinitz sur les espaces de matrices (7’53’’) Un développement de Tiphaine (agrégative) sur l'action de Steinitz sur les matrices dont les orbites sont classifiées par le rang. Lorsque l'on est sur R ou C, on peut comprendre les adhérences d'orbites pour cette action.

Optimiser l'aire d'un triangle inscrit dans deux cercles tangents par Sam (16’09’’) Sam nous présente un petit développement qui mêle savamment, cercles, triangles, géométrie, calcul différentiel, trigonométrie et topologie… Référence : le Karmati.

Construction à la règle et au compas du p-gone régulier par Loris (27’15’’) 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 (18'10'') 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-Wantzel pour ceux qui connaissent un peu la théorie de Galois.

Probabilité pour que deux éléments commutent dans un groupe fini (18'06'') 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 $GL_2(K)$ (18'31'') 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 $GL_n(K)$ (22'50'') On vient de calculer la probabilité pour que deux matrices de $GL_2(K)$ commutent sur un corps fini K. La généralisation de ce résultat à $GL_n(K)$ 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.

Irrationnalité de Pi par Riri (14'14'')

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 !

Points remarquables du triangle et barycentres (15'01'')

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.

Questions d'oral (26)

Question de jury sur la leçon 106- Groupe linéaires-Sous-groupes (14'57'') 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**.

Questions de jury sur le thème racines de l'unité (14'32'') 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 ϕ_n sur Q et leur degré ϕ (n). 2) Le fait que ϕ (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.

Question de jury - Leçon PGCD ou rang-dimension (14'05'') 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 ?

Question de jury sur le thème distances ou extrema (12'19'') On trouve, en algèbre comme en analyse, à l'interne 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 !

Questions de jury autour du rang en algèbre linéaire (34'11'') 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**. Et, à la fin, une rencontre du troisième type :-) ! Puis quelques questions classiques sur **les propriétés topologiques du rang.** Enfin, une dernière question de jury autour des propriétés du rang, mais, cette fois-ci, **le rang concerne les formes quadratiques sur un corps fini** !

Question d'oral à l'AE (Anneaux et corps) -1 (17'44'') 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...
Question d'oral à l'AE (Anneaux et corps) -1bis (17'10'') L'injection du groupe $GL_n(F_{p^2})$ dans $GL_{2n}(F_p)$ 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 F_{p^2} est un corps, en se concentrant uniquement sur sa structure de F_p espace. C'est peut-être dans ce lâcher prise que réside toute la difficulté...
Question d'oral à l'AE (Anneaux et corps) -2 (16'44'') Ici, il sera question de polynômes annulateurs d'un entier algébrique, irréductibilité, 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 Z se décompose modulo p pour tout p. On passera, ensuite, en revue les corps algébriquement clos à connaître pour l'oral.
Question d'oral à l'AE (Anneaux et corps) -3 (15'08'') 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.

Question d'oral à l'AE (Réciprocité quadratique) -1 (9'27'') Toujours dans la série des questions de jury. Quelles sont les thèmes développés autour de la réciprocité quadratique ?
Question d'oral à l'AE (Réciprocité quadratique) -2 (14'15'') 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.

Question d'oral à l'AE (Groupes finis) -1 (19'19'') 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. Ensuite, toujours lié au théorème de structure, l'omniprésence des groupes cycliques nous entraîne vers l'étude des homomorphismes entre Z/nZ et Z/mZ. 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 et passage au quotient).
Question d'oral à l'AE (Groupes finis) -2 (21'45'') 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.
Question d'oral à l'AE (Groupes finis) -3 (15'39'') 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.
Question d'oral à l'AE (Groupes finis) -4 (18'51'') 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 $GL_n(F_p)$.

Question d'oral à l'AE (Algèbre linéaire) -1 (10'12'') 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.
Question d'oral à l'AE (Algèbre linéaire) -2 (19'11'') 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.
Question d'oral à l'AE (Algèbre linéaire) -3 (13'48'') Quelques questions de jury pour tester des réflexes sur les problèmes de dimensions d'espaces vectoriels.

Question d'oral à l'AE (Algèbre linéaire) -4 (19’28’’) 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.

Question d'oral à l'AE (Algèbre linéaire) -5 (12’16’’) 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.

Question d'oral à l'AE (Algèbre linéaire) -6 (13’33’’) 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.

Question d'oral à l'AE (Algèbre linéaire) -7 (15’57’’) 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.

Question d'oral à l'AE (Algèbre linéaire) -8 (11’39’’) 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 C, 2. sur ses matrices diagonales, 3. sur ses matrices diagonalisables et enfin, sur $M_n(C)$ tout entier.

Question d'oral à l'AE (Algèbre linéaire) -9 (19’49’’) 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.

Question d'oral à l'AE (Algèbre linéaire) -10 (17’25’’) 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.

Question d'oral à l'AE (Arithmétique) (13’33’’) Deux petits exercices étonnants autour d'une leçon sur les anneaux factoriels. Un qui illustre une application de l'anneau factoriel Z[i] et l'autre, plus simple, est une application du critère d'irréductibilité d'Eisenstein.

Divertissements mathématiques (104)

Cinq preuves coup de cœur pour une infinité de nombres premiers (27'15'')

On propose **5 preuves, toutes d'horizons totalement différents, pour l'infinitude de l'ensemble des nombres premiers** (et la bravitude de leurs auteurs !)

00:00 Introduction 01:43 **Preuve historique** 05:02 **Preuve arithmétique** 10:23 **Preuve par les groupes** 12:33 **Preuve analytique** 20:58 **Preuve topologique**

Localisation des racines d'un polynôme (une brève histoire) (25'56'')

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 faites, **on attaque le théorème de Enestrom-Kakeya, ses corollaires ainsi que ses développements plus récents**.

Localisation des racines d'un polynôme-addendum (7'20'')

Suite à une remarque de @totototo8119, 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 @totototo8119 : on peut trouver la preuve dans le livre "**Petit compagnon des nombres et de leurs applications" de Pascal Boyer** p. 349 (avec la matrice compagnon, on pouvait s'y attendre !)

Le théorème du confinement (29'22'')

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**.

Peut-on couper un gâteau (polygonal) en 6 parts égales avec trois coups de couteau ? (13'32'') 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**.

Equation diophantienne aux Olympiades (10'09'')

Une petite équation diophantienne astucieuse qui demande juste un niveau "terminale option maths" mais, surtout, beaucoup d'amour et de passion...

Equation diophantienne, estivale... et cyclotomique (12'40'')

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.**

Un petit exercice d'arithmétique (équation diophantienne) (3'43'')

Un tout petit exercice d'arithmétique que m'a proposé mon ami Rached Mneimné **sur la somme des carrés d'entiers consécutifs.**

Exercice Oraux X-ENS : quand le groupe d'automorphismes d'un groupe est-il trivial ? (10'32'')

Un exercice donné 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.

Un 2-Sylow de S_4 en 6ème avec l'IREM (20'13'')

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.

Décimales et groupes cycliques - le nombre 142857 et ses amis (25'03'')

Voici un petit tour de magie, à la Gérard Majax, qui fait intervenir groupes cycliques et décimales.

Les invités du Capitaine Woody (16'38'')

Un petit quizz autour d'un problème mondain lors d'une croisière sur le paquebot du Capitaine Woody.

Une preuve sans mot (relativement très connue) (4'18'')

Arriverez-vous à entendre ce que ces trois triangles veulent vous dire ? Une preuve sans mot proposée par Jérôme Germoni

Quel est l'âge d'Esteban (el Capitan) ? (24'33'') 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 !

Le p-adique (ses merveilleuses applications) (48'19'')

L'épreuve 1 de l'agrégation interne 2023 nous invite (maladroitement, certes) à nous intéresser aux **entiers p-adiques**. Nous allons introduire, de façon piétonne, **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 (Définition de l'anneau Z_p, valuation et distance ultra-métrique, inversibles de l'anneau Z_p, topologie de Z_p et application). http://mathem-all.fr/bw/introductiona...

Dernières décimales de $n^{\{10^{\wedge}d\}}$ (aux olympiades ou plus si affinités) (6'58'')

Un petit exercice d'olympiades en arithmétique. Au programme : **congruence, indicatrice d'Euler et groupe des inversibles de l'anneau (Z/nZ)***

Minoration de la fonction π de comptage des nombres premiers (Capes 2008) (22’43’’)
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 !
Majoration de la fonction π de comptage des nombres premiers (12’33’’)
Après avoir minoré la fonction π 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 π à peu de frais**.

Entiers consécutifs avec/sans facteurs carrés ? (5’11’’) Tout est dans le titre. Peut-on **trouver des suites d'entiers consécutifs (avec/sans) facteurs carrés aussi longues que l'on veut**.
007 contre S_{26} (12’56’’) Voici **un exercice récréatif qui permettra de réviser nos classiques sur le cours groupes et anneaux (groupe de permutation, anneau Z/nZ)**. Cet exercice est extrait du site les mathematiques.net et a été proposé par GaBuZoMeu.

Devinez la caractéristique du corps ! (10’06’’) Un petit exercice taquin pour occuper nos méninges ! Soit a_i, i de 1 à 27 des éléments non nuls d'un corps 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 K.

Ampoules et interrupteurs en caractéristique 2 (1h11’17’’) Une histoire d'ampoules et d'interrupteurs... et de **formes quadratiques sur le corps F_2** !

Pavage d'un ballon de foot par des hexagones ? (12’20’’) 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 $PSL_2(F_7)$ et $PGL_3(F_2)$.**

Un problème de cinéphile ! (7’15’’) Petit problème ludique de géométrie dans une salle de cinéma !

Doctor Fibonacci, I presume ? (7’31’’) 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**.

Popcorn maths 'n burger quizz (5’12’’) Le petit quizz du jour qui **se joue avec cinq nombres réels**.

Le corbeau et le renard, une fable mathématique (6’11’’) 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 ? La prochaine fois, nous verrons le corbeau et le renard en langage inclusif. P.S. Après avoir posté la vidéo, j'ai reçu **un message de l'auteur. Il s'agit de Mickael Launay**. Merci à lui pour cette fine analyse de texte, cette fidèle traduction et ce bel hommage à Monsieur de la Fontaine.

Des vœux de bonne année selon une tradition familiale... (19’41’’) ... dans les familles de mathématicien ! 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 !

Maths et Pizzas (8’44’’) Nous parcourons ici une brève histoire de la pizza et sur la façon dont les mathématiciens ont abordé, du XVIIème siècle à nos jours, les problèmes liés à cette invention majeure de l'humanité.
U-Turn (Philippe) par Guillaume Mallet (3’32’’) Une belle année de prépa pleine d'émotions, qui finit en chanson, avec Guillaume et sa cover de U-Turn (Lili)
Tarare (et on a fait des maths) (3’39’’) A joint work of U.C.B.L (United Choir of Baire Lovers) and Topoldavy University
La dernière échéance, United Choir of Baire Lovers (4’15’’) Une petite vidéo souvenir de ces moments passés à préparer l'agreg externe sous confinement

**

Factorisez X^{16}-X en irréductibles sur le corps à deux éléments (14’18’’) Un exercice instructif qui nous oblige à bien maitriser la théorie des corps finis.
Factorisez X^{16}-X en irréductibles sur le corps à deux éléments-2 (14’30’’) 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**.

Sous-espaces stables et idéaux de K[X] (18’39’’) 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**.
5 est-il un carré modulo p ? (17’35’’) Nous venons de voir dans une vidéo précédente **que 2 est un carré [p] (différent de 2) ssi p ≡ 1 ou -1[8]**. Nous allons voir une méthode très analogue qui nous montre que **5 est un carré [p] (différent de 5) ssi p ≡ 1 ou -1[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.**
x^3+7 peut-il être un carré? (15’52’’) 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**.

Critères de simplicité d'Iwasawa pour u groupe-1/2 (20'25'') et Critères de simplicité d'Iwasawa pour un groupe-2/2 (18'04'') Qui aurait pu prévoir un lien entre simplicité d'un groupe et multi-transitivité d'une action fidèle ? Et bien Iwasawa a ouvert une voie royale entre les deux notions. On montre un lemme préliminaire puis un critère de simplicité pour un groupe à action multi-transitive à stabilisateur simple. Et c'est simple... comme bonjour !

Galois et la non résolubilité par radicaux (39'44'') Comment Evariste Galois a pu prouver cette non résolubilité par radicaux de certaines équations, en degré 5, là 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.

Le témoin de Solovay-Strassen - Un test de primalité (14'04'') 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.

La loi de réciprocité d'Artin-1 (39'11'') 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 cœur de l'arithmétique et, tout particulièrement, de la théorie du corps de classes.

La loi de réciprocité d'Artin-2 (22'39'') 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[p].

La loi de réciprocité d'Artin-3 (35'43'') On va regarder de près deux exemples-clef : 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 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.

La loi de réciprocité d'Artin-4 (33'01'') 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 Z et une version pour les entiers de corps de nombres qui nous amène à construire le "ray class group".

Le lemme d'Artin ou l'invitation à la théorie de Galois (14'26'') 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.

Le nombre 20160 et un non-isomorphisme exceptionnel-1 (15'07'') 20160, 196884 et quelques monstres... Nous allons aujourd'hui parler de coïncidences numériques et, en particulier, parmi les ordres des groupes simples.

Le nombre 20160 et un non-isomorphisme exceptionnel-2 (13'54'') On montre ce scandaleux résultat que, malgré les indices et les apparences, les deux groupes simples $GL_3(F_4)$ et $GL_4(F_2)$ 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.

Une (petite) identité de Ramanujan (8'43'') 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.

La formule du binôme quantique (26'22'') 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.

Le théorème (fort) de progression arithmétique de Dirichlet (43'45'') 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 [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.

Théorème de progression arithmétique : une preuve en 10 minutes ? (16'17'') 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.

Un tour de magie (avec des nombres binaires !) (4'28'') Nous recevons la visite de notre ami Antoine qui nous propose un tour de magie avec les nombres binaires.

Le théorème de meilleure approximation rationnelle (26'56'') 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 petite 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.

$x^2 \equiv x$ [10^k] ou les rimes de la multiplication (28'46'') Cinq fois cinq vingt-cinq, six fois six trente-six mais sept fois sept ne font pas quarante-sept. Comment ça a pu partir 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 Z/nZ.

Irréductibilité dans Z[X] par congruence (15'45'') Une situation classique où l'on veut montrer qu'un certain polynôme à coefficients entiers est irréductible sur 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... Errata: Juste à la fin il aurait fallu dire que a n'est pas multiple de p.

ζ(2) - Les plus belles preuves ! (38'59'') **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/ba...
#5 Méthode des résidus - #4 Série de Fourier - #3 Taylor et Wallis - #2 Intégration- le changement de variables qui tue - #1 Points entiers de la 4-sphère

Une devinette polynomiale (5'15'') **Une devinette, proposée par Daniel Juteau, où l'on doit deviner un polynôme en deux questions alors qu'on ne sait même pas son degré !**
Des formules non polynomiales pour les nombres premiers ! (11'06'') On présente ici **deux formules explicites amusantes, une formule donnant le nième premier et une autre formule donnant le nombre de nombres premiers plus petits que n**.
Des formules polynomiales pour les nombres premiers ? (11'32'') 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.
Une preuve d'Erdos sur la localisation des nombres premiers (29'29'') Un petit exercice fortement inspiré de "A fun number theory problem" de Dr Barker, A Fun Number Theo... 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**".

Distribution des puissances en base 10 et loi de Benford (1h13'08'')
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 puissances de 3, sans oublier les nombres de Fibonacci. Pour l'instant, pas de preuve mais un premier énoncé.
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 une 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.
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 $e^{2s/piak}$, k de 1 à n, tend vers 0.
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**.
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 $5^5=3125$.

Equations grégophantiennes-1 (14'47'') 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 ?
Equations grégophantiennes-2 (16'28'') **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".
Equations grégophantiennes-3 (9'49'') On finit par résoudre l'énigme du Dimanche 21 avril. Étonnamment, c'est **un système de congruence** qui va nous y amener.

2021 et le jour de π-1 (13'29'') La racine carrée de 98723 est 314,2021..., ce qui en fait un nombre emblématique pour le jour de **π**. 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.
2021 et le jour de π -2 (11'39'') 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.**
2021 et le jour de π -3 (22'27'') Et la lumière fut ! **On utilise le groupe $GL_2(Z)$ pour voir plus finement les choses sans changer la nature entière du problème**. On retrouve toutes les solutions avec aisance et un minimum de calcul.

Suites de presqu'entiers et nombres de Pisot-1 (14'30'') 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"**.
Suites de presqu'entiers et nombres de Pisot-2 (12'42'') 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**.
Résolution d'un système de Vandermonde (et nombres de Pisot-3) (13'59'') Les mathématiciens confirmés connaissent par cœur **la formule du déterminant de Vandermonde** mais peu d'entre eux savent **inverser la matrice de Vandermonde**. **Une astuce utilisant les polynômes permet de le faire élégamment**. On aura ensuite besoin de cette inversion pour montrer le théorème de Pisot dans une prochaine vidéo.
Suites de presqu'entiers et nombres de Pisot-4 (21'48'') On prouve **le théorème de Pisot. Un nombre algébrique réel > 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 Z^n, morphisme de multiplication dans un anneau et morphismes de conjugaison dans un corps).**

Le théorème de Fermat de taille moyenne 1 (14'57'') **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...

Le théorème de Fermat de taille moyenne 2 (12'30'') 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**.

Le théorème de Bruck-Ryser (26'51'') 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! 😩

Fonctions absolument continues par Tristan (53'14'') 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.**

L'escalier du diable par Tristan (23'34'') 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.**

Le corps C est algébriquement clos. Ma preuve coup de cœur ! (14'31'') 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 **!**

Théorème de représentation d'une fonction lipschitzienne par Tristan (32'25'')

Tristan nous propose un théorème haut en couleur qui prouve que **toute fonction lipschitzienne u sur R peut être représentée par une fonction g dans L^∞(R) dans le sens : u(y)-u(x)= $\int_x^y g(t)dt$.**

Le théorème de Borsuk-Ulam ou la rencontre des pôles-1 (8'01'')

Peut-on trouver, à chaque instant, sur Terre, deux points antipodiques avec exactement la même température et la même pression ? Eh 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 il 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 !

Le théorème de Borsuk-Ulam ou la rencontre des pôles-2 (13'55'')

La suite des aventures **en dimension 2**.

Le théorème de Fejér prouvé par Korovkin (23'07'') 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 qu'u_n(f) converge uniformément vers f, pour f=1, cos et sin !** Référence : Hirsch-Lacombe p. 33.

Théorème de Kronecker. La preuve la plus simple ? (10'53'') Voici, à un niveau où le prérequis 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 Z[X] ayant toutes ses racines de normes inférieures ou égales à 1, possède des racines soient nulles soient racines nièmes de l'unité**.

Les projecteurs spectraux par l'analyse complexe (19'01'') Un étudiant de licence de mathématiques a rencontré **les projecteurs spectraux**, les mêmes **qui permettent de montrer le lemme des noyaux**. Toutefois, il les a, en général, **vus dans le contexte de l'arithmétique avec l'identité de Bézout.** 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**.

Rudiments de théorie de Minkowski pour l'agrégation (15'32'') 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 R^n. Voici une présentation minimaliste de la théorie.

Un fractal de Pascal (43'27'') Pour le $400^{ème}$ anniversaire de Blaise Pascal, 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 autosimilarité tensorielle...** On prouve ensuite la propriété d'autosimilarité tensorielle du triangle de Pascal modulo un nombre premier p, qui donnera 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'autosimilarité 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).

Divine proportion, nombre plastique et méthode des puissances (48'34'') 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 (ou pas) 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 complexes. 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**.

Triangles équilatéraux et nombre d'or (21'34'') 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 égalité 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 affixe, qui a permis à Jean-Jacques d'intégrer la construction dans la rétine du héros de manga Itachi Uchiwa.

Triangles équilatéraux et nombre d'or-2 (11'11'') 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.

Variance des inversions, polynômes générateurs et décomposition de Bruhat (23'51'') 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 !)

Un paquet cadeau, c'est pour offrir ! (32'29'') On veut montrer qu'un compact convexe X de 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.

Concours SMF-Junior 2022-Algèbre (41'01'') **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)**.

Le théorème de Polya sur les coloriages (35'27'') **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...

Le théorème de Cartan-Von Neumann (40'46'') **Le théorème de Cartan Von Neumann (ou tout simplement de Cartan) dit qu'un sous-groupe fermé du groupe $GL_n(R)$ possède une structure de sous-variété de $M_n(R)$.** 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 !

L'image de l'exponentielle réelle. On fait le point (barre) ! (24'15'') On présente **tous 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.

Le théorème à la fin heureuse - la preuve de Paul Erdös (26'45'') 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...

La conjecture de sensitivité par Corentin Faipeur-1 (12'32'') 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 30 années de résistance.

La conjecture de sensitivité par Corentin Faipeur-2 (17'39'') 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.

La conjecture de sensitivité par Corentin Faipeur-3 (19'35'') **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 au principe du min-max (44'51'') (partie III).

Dessins d'enfants par Alex Moriani-1 (24'09'') 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.

Dessins d'enfants par Alex Moriani-2 (20'31'') Voici une présentation (sans preuves mais avec illustration !) **des résultats de Belyi et Grothendieck autour des dessins d'enfan**

Fibration de Hopf (par les quaternions) (31'58'')
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 !**

Lemme du ping-pong et groupe modulaire (19'44'')
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**.

Application de la cyclicité de (Z/pZ)*: les nombres de Giuga (18'06'')
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**.

C'est graphe docteur ? (7)

Graphes (a minima) pour l'oral de l'agrégation-1 (18'31'') 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 algorithmes, on attaque le lemme des poignées de mains, avec un joli problème... de poignées de mains.
Graphes (a minima) pour l'oral de l'agrégation-2 (17'35'') On regarde **les longueurs de chemins, le long des arêtes d'un graphe**, ce qui nous amène naturellement du côté théorique, vers des problèmes 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 empêché de gagner le mondial en 1998...
Graphes (a minima) pour l'oral de l'agrégation-3 (8'31'') On termine avec quelques petites choses sur **le nombre chromatique** et des petites choses afférentes.

Nombre chromatique d'un graphe et théorème spectral (23'06'') **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.

Inégalités de Cheeger pour les graphes (30'13'') **L'étude des graphes 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**.

Un exercice sur les graphes et la star ζ (2) ! (22'30'') Voici un exercice assez élémentaire sur la coloration des graphes qui fera curieusement intervenir la fonction **ζ** (2) et donc le fameux nombre **π**. 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.

Combinatoire et placements de table (12'55'') 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 !)

****

**