Playlists et Vidéos Youtube

Le collier de perles (6 vidéos) *(formule de Burnside, $\mathbb{Z}/4\mathbb{Z}$, cas général Cyclique, D_n)*

On va essayer de ne pas se rouiller pendant cette période de confinement ! Voici une présentation (un peu improvisée de par la soudaineté des évènements) du collier de perles en trois parties, suivie d'un épilogue. Il s'agit de problèmes de dénombrement par action d'un groupe cyclique. Sur la fin, on donne des indications pour l'action du groupe diédral.

Vidéo 5 : On répond à une question très naturelle des coloriages du n-gone modulo isométries, et non plus modulo rotations.

Vidéo 6 : On répond à une question très naturelle des coloriages du n-gone modulo isométries et non plus modulo rotations. Ceci nous amène à observer le groupe diédral. On finit sur une formule générale du nombre de coloriages, qui distingue le cas pair et le cas impair.

Formes de Hankel (7 vidéos) *(du cas où P n'a que des racines réelles au cas général)*

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

Vidéo 1 : Pour l'étude d'un cas élémentaire, où les racines sont toutes réelles et distinctes, et la forme de Hankel est définie positive.

Vidéo 2 : Pour l'étude d'un autre cas élémentaire, où les racines sont toutes réelles mais non forcément distinctes, et la forme de Hankel est positive.

Vidéo 3 : Pour trouver la matrice de la forme de Hankel.

Vidéo 4 : Cette fois-ci, les nombres α_i ne sont plus forcément ni distincts ni réels, mais s'il ne sont pas réels, ils seront conjugués.

Vidéo 5 : On va ici, enfin (il était temps !), définir la forme de Hankel associée à un polynôme réel en toute généralité.

Vidéo 6 : On veut dans cette vidéo calculer la signature de la forme de Hankel associée à un polynôme réel T.

Vidéo 7 : 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.

Compter avec les groupes (8 vidéos) *(la formule de la classe, S_n, nombres multinomiaux, $\mathrm{GL}_n(\mathbb{F}_p)$, sous-espaces en somme directe, matrices diagonalisables)*

On va montrer dans une série de vidéos 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.

Vidéo 2 : Dans cette vidéo, 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).

Vidéo 3 : On passe facilement du groupe symétrique au groupe linéaire en remplaçant "sous-ensembles" par "sous-espaces" et "partitions" par "sous-espaces en somme directe". On obtient des dénombrements où les factorielles sont remplacées par des cardinaux de groupes linéaires sur un corps fini.

Vidéo 4 : On s'attaque au nombre de matrices diagonalisables sur un corps fini. On obtient une jolie formule.

Vidéo 5 : La formule obtenue pour dénombrer les matrices diagonalisables était jolie, mais peu utile en l'état. Elle comportait trop de termes quand le corps devenait 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.

Vidéo 6 : On veut compter le nombre de matrices de rang r sur un corps fini. Pour l'instant, on se contente d'un calcul préliminaire : celui du calcul du nombre de sous-espaces de dimension k fixée.

Vidéo 7 : 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.

Vidéo 8 : 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.

Le groupe orthogonal (4 vidéos) *(générateurs de O_n, de SO_n, SO_3 est simple)*

On étudie le groupe orthogonal d'un espace euclidien.

Vidéo 1 : On s'intéresse à l'engendrement du groupe orthogonal par des réflexions orthogonales.

Vidéo 2 : Dans cette vidéo, on montre le résultat classique de l'engendrement du groupe spécial orthogonal par des retournements orthogonaux.

Vidéo 3 : On attaque ici la simplicité de SO_3. Il ne faudra pas moins de deux vidéos pour en venir à bout.

Vidéo 4 : Dans cette dernière vidéo, on parachève la preuve de la simplicité de SO_3.

Structures quotients (7 vidéos) *(structure quotient ensembliste, passage au quotient, groupe, quotient et théorème de Lagrange, groupe quotient, sous-espaces quotient : formule du rang et noyaux emboîtés, idéaux, passage au quotient, lemme chinois, équations diophantiennes avec 31)*

Il s'agit d'une série de vidéos où on présente les structures quotient dans le programme universitaire.

Vidéo 1 : On montre qu'une application est une bijection qui s'ignore.

Vidéo 2 : Dans cette vidéo, on présente le quotient d'un groupe par un sous-groupe non nécessairement distingué.

Vidéo 3 : On montre ici comment obtenir des structures de groupes quotient à l'aide d'un sous-groupe distingué.

Vidéo 4 : On s'attaque maintenant aux structures d'espaces 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.

Vidéo 5 : Une preuve élégante (mais classique !) de l'essoufflement de la suite des noyaux emboîtés est présentée. Elle utilise le passage au quotient.

Vidéo 6 : On se dirige maintenant vers l'arithmétique en introduisant les idéaux. Ceux-ci permettent de construire des structures d'anneaux quotient, tout en généralisant la relation "divise" des entiers.

Vidéo 7 : Dans cette dernière vidéo, on montre comment les structures quotient peuvent amener à résoudre des équations diophantiennes.

Le théorème du confinement (2 vidéos) *(pièce cylindrique à n personnes, comment se tenir assez éloigné, preuve de l'inégalité d'Hadamard et cas d'égalité)*

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.

Droites, cercles et homographies (5 vidéos) *(cocyclicité, birapport, homographies, préserver le birapport, les droites ou cercles, transitivité de l'action, inégalité de Ptolémée)*

Les droites et cercles du plan sont étudiées à l'aide du calcul complexe, du groupe des homographies... et du birapport.

Vidéo 1 : 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.

Vidéo 2 : On présente maintenant le groupe des homographies. Il s'agit d'un groupe de transformations qui contient les translations, les similitudes directes et qui va préserver les cercles et droites. "Oui, mais quand ?" comme dit mon collègue préféré. Et bien quand vous serez prêts à le regarder en face !

Vidéo 3 : 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.

Vidéo 4 : Dans cette vidéo, on montre que le groupe des homographies agit de façon transitive sur l'ensemble des "cercles et droites".

Vidéo 5 : On montre ici l'inégalité de Ptolémée et son cas d'égalité, qui caractérise les quadruplets de points inscriptibles sur un cercle à l'aide des distances entre ces points. Encore une fois, le birapport est en première ligne.

Ellipse de Steiner (6 vidéos) *(Existence, unicité, foyers de l'ellipse)*

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.

Vidéo 2 : 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.

Vidéo 3 : On aborde le problème des foyers de l'ellipse de Steiner. Pour l'instant, on ne fait qu'évoquer Gauss-Lucas et montrer que seul le groupe des isométries peut nous apporter quelque chose. Peu, mais ce sera suffisant pour démarrer. 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.

Vidéo 4 : On introduit sous forme complexe une transformation affine.

Vidéo 5 : On est en mesure de calculer l'équation de l'ellipse sous une forme dont on sait déduire les foyers.

Vidéo 6 : A l'aide l'équation de l'ellipse de Steiner, on en calcule les foyers et on vérifie à l'aide de relations coefficients/racines qu'ils coïncident avec les racines du polynôme dérivé du triangle de départ.

Théorie des représentations (19 vidéos) *(Théorie des représentations, construction d'une table de caractères, le cas S_4, toutes les interprétations des irréductibles de S_4)*

Vidéo 1 : Un mini-cours en théorie des représentations complexes de groupes finis. On commence par tester 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.

Vidéo 2 : On continue avec l'étude "à la main" de la théorie des représentations. rien de tel que le système D pour forger un "caractère". On passe au groupe $\mathbb{Z}/3\mathbb{Z}$ qui nous permet de comprendre ce qui se passe pour tout groupe cyclique, puis le premier groupe non abélien S_3.

Vidéo 3 : On définit les représentations, les morphismes de représentations, et on montre le théorème de Maschke.

Vidéo 4 : On s'attaque à la classification des représentations d'un groupe. Par Maschke, on voit qu'il suffit de trouver toutes les représentations irréductibles. Elles se trouvent toutes dans la représentation dite régulière du groupe, qui est un cas particulier de représentation par permutation.

Vidéo 5 : On prouve ici le théorème d'orthonormalité des caractères avant d'en découvrir les multiples corollaires.

Vidéo 6 : On donne ici les conséquences théoriques du résultat de Schur qui dit que les caractères irréductibles forment une base orthonormée de l'espace des fonctions centrales sur le groupe. On va voir que le caractère caractérise la représentation à isomorphisme près.

Vidéo 7 : Après avoir vu les conséquences théoriques du théorème de Schur sur la base unitaire des caractères, nous en découvrons les côtés pratiques avec tout un univers de petites recettes pratiques qui contribuent au bonheur et à l'harmonie dans la belle algèbre.

Vidéo 8 : Un préambule important avant d'attaquer la construction des tables de caractères : comment tirer parti d'une action de groupe pour en extraire un caractère irréductible qui figurera sur une ligne du tableau ?

Vidéo 9 : On commence à construire des tables de caractères. Pour se mettre en jambes : la table du groupe cyclique et celle du groupe symétrique S_3.

Vidéo 10 : La table de caractères du groupe S_4 a la taille parfaite pour 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.

Vidéo 11 : On commence à donner un sens plus empirique à toutes les représentations irréductibles de S_4. Action de groupes et tensorisation par la signature sont les mots clef.

Vidéo 12 : Cette fois on réinterprète la table de caractères de S_4 en termes géométriques. Pour cela, on réalise S_4 d'une part comme groupe d'isométries du tétraèdre régulier, d'autre part comme groupe d'isométries positives du cube.

Vidéo 13 : On attaque une nouvelle série où l'on part de la table de caractères du groupe et où on en trouve des explications. Après un petit briefing sur le schéma général de ces applications dans divers domaines, on regarde sur des exemples où l'on calcule des multiplicités de représentations irréductibles dans une représentation donnée.

Vidéo 14 : On continue des exemples géométriques où il fait sens de décomposer une représentation en irréductibles. Un, avec les quadrilatères du plan, muni de l'action cyclique, et un autre, avec l'action des rotations du cube sur des faces.

Vidéo 15 : On prépare une petite extension du lemme de Schur dans le cas où la représentations n'est pas nécessairement irréductible mais seulement sans multiplicité.

Cela va nous permettre par la suite (vidéos 16 et 17) de présenter de l'analyse harmonique discrète (mais non moins élégante !)

Vidéo 16 : On présente ici une version du théorème de Thébault par la théorie des représentations. La construction d'un carré à partir d'un parallélogramme peut se comprendre facilement si l'on voit cette construction comme un morphisme de représentations dont l'image est l'espace des carrés par une version modifiée du lemme de Schur vue dans la vidéo précédente. Le théorème de Napoléon est également discuté sous le même angle de l'analyse harmonique.

Vidéo 17 : On termine ce petit volet sur l'analyse harmonique avec l'exemple classique de A.A. Kirillov déjà présenté dans la vidéo 14. Il s'agit d'un exemple simple permettant d'indiquer comment la théorie des représentations s'est introduite dans la physique, liée aux transformations linéaires conservant une certaine structure.

Vidéo 18 : On attaque maintenant un nouveau volet sur ce que disent les tables de caractères de G sur le groupe fini G. Il se trouve que l'on va pourvoir retrouver tous les sous-groupes distingués de G. On regardera dans une prochaine vidéo des sous-groupes distingués particuliers comme le centre et le groupe dérivé.

Vidéo 19 : On montre de façon pratique de façon théorique, puis sur des exemples, comment tirer le centre et le groupe dérivé de table de caractères.

Structure de groupe sur une conique (9 vidéos) *(classification des coniques, puis des coniques munies d'un point, ce qui se passe en forme normale, cas général, l'hexagramme mystique, les courbes elliptiques)*

Vidéo 1 : Voici une petite série de vidéos où l'on présente une construction de groupe sur les coniques. Il s'agit d'une construction qui fait le point sur des propriétés géométriques des coniques bien cônues depuis Pascal, et dont les applications à la cryptographie (que l'on effleurera seulement) sont apparues de façon relativement récente. Cette première vidéo est avant tout un teaser.

Vidéo 2 : Dans cette vidéo, on donne la construction générale pour la structure de groupe sur une conique non dégénérée. On montre que l'on a bien un groupe dans trois cas particuliers. Et ces groupes ne sont pas anodins. Il s'agit du groupe additif (pour la parabole), du groupe multiplicatif (pour l'hyperbole), et le groupe additif modulaire, comme les groupe des angles, (pour l'ellipse). Si on ajoute à cela que ces groupes géométriques sont à la fondation de la cryptographie actuelle, on se dit qu'il n'y a que les maths pour nous faire traverser, dans une logique implacable, l'histoire antique, notre monde actuel, et les souvenirs nostalgiques des premières opérations de notre enfance.

Vidéo 3 : 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 !

Vidéo 4 : 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.

Vidéo 5 : On finit ici la preuve du théorème de classification des coniques non dégénérées par les trois groupes classiques réels.

Vidéo 6 : On a montré le théorème de structure de groupe sur une conique, à l'aide d'un mélange de petit calculs dans trois cas simples et de groupes de transformations. On veut maintenant une preuve plus directe en travaillant sur la géométrie de la conique. L'associativité pose un petit problème, qui va être résolu grâce au théorème de l'hexagramme mystique de Pascal.

Vidéo 7 : 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.

Vidéo 8 : On pensait s'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.

Vidéo 9 : Dernier volet de la série où l'on montre (en mode DSK) comment les coniques, en leur ajoutant une droite, sont des dégénérescences d'une famille de courbes elliptiques. On finit sur des explications (à détailler avec de bonnes références !) sur les applications de ces dernières à la cryptanalyse et à la cryptographie.

Exercices sur les formes quadratiques (8 vidéos)

Vidéo 1 : Une généralisation de la formule d'Apollonius, deux exercices sur le gonflement hyperbolique, principe du min-max de Rayleigh, image d'une sphère par une surjection de $\mathbb{R}^3$ sur $\mathbb{R}^2$, deux vidéos sur l'étude affine des coniques à partir de leur équation cartésienne, les formes quadratiques entières binaires qui servent à voir si deux matrices sont $\mathbb{Z}$-semblables.

Vidéo 2 : 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".

Vidéo 3 : On va se servir du gonflement hyperbolique dans un cas simple : soit E un espace réel muni d'une forme quadratique non dégénérée q, on veut montrer que le groupe des isométries de q agit transitivement sur l'ensemble des vecteurs isotropes non nuls de E. Comment faisait-on pour montrer que O_n agit transitivement sur la sphère, on prenait un élément de norme 1 et on le compétait en une base orthonormée. Là, c'est pareil, sauf qu'il n'y a pas de base orthonormée.

Vidéo 4 : On présente progressivement le principe de Rayleigh ou principe du minimax en petite dimension. Il s'agit d'une caractérisation géométrique des valeurs propres. On en donne une application amusante sur une fonction trigonométrique.

Vidéo 5 : 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.

Vidéo 6 : 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.

Vidéo 7 : 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 homogénéisée provenant de l'équation de départ.

Vidéo 8 : On connaissait un lien fort entre formes quadratiques et réduction avec le théorème spectral. En voici un autre en arithmétique qui permet de voir si deux matrices de $M_2(\mathbb{Z})$ sont $\mathbb{Z}$-semblables en leur associant des formes quadratiques. La $\mathbb{Z}$-similitude s'interprète alors sous forme de congruence des formes quadratiques.

Exercices en Arithmétique (12 vidéos) *(Equations diophantiennes $x^2+y^2-29z^2=0$, $x^2+y^2-31z^2=0$, divisibilité d'un nombre de Fibonacci par un nombre premier, nombre d'automorphismes polynomiaux en une matrice fixée sur un corps fini, cardinal de $\mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$, divisibilité d'un nombre de Fibonacci par un nombre m, en particulier, n tel que F_n se termine par k zéros en décimal, équation de Pell-Fermat et structure de groupe monogène, puis équation de Pell-Fermat et fractions continues, puis la bataille de hastings : $x^2-13y^2=1$, le problème du nombre de racines m-ièmes d'une matrice compagnon avec le lemme de Hensel)*

Vidéo 1 : On résout ici l'équation diophantienne $x^2+y^2-29z^2=0$ en mettant l'accent sur la factorialité de l'anneau $\mathbb{Z}[i]$ des entiers de Gauss.

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

Vidéo 3 : On avait déjà vu dans une vidéo sur les "Structures quotient" que $x^2+y^2-31z^2=0$ avait pour seule solution $(0,0,0)$. Ici, on le montre à la suite de la vidéo "Arithmétique 1" comme application immédiate de la factorialité de l'anneau $\mathbb{Z}[i]$ des entiers de Gauss.

Vidéo 4 : 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 telle que p divise F_n si et seulement si (p) divise n... Et nous voici embarqués dans de curieuses considérations de savoir si 5 est un carré modulo p. Pas si curieuses au final, si l'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 $b^2 + ab - a^2 = (b + a/2)^2 - 5(a/2)^2$.

Vidéo 5 : 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.

Vidéo 5 : Voici un autre exercice sur le lemme chinois. Cette fois-ci on le retrouve dans une version matricielle. Ceci permet de calculer le nombre de matrices inversibles de taille d sur l'anneau $\mathbb{Z}/m\mathbb{Z}$.

Vidéo 6 : Dans la vidéo Arithmétique 3, on regardait le problème de connaître l'ensemble des entiers n tels que le nombre de Fibonacci F_n soit divisible par un entier premier p. On passe maintenant du nombre premier p à un nombre entier quelconque m. On tombe sur une fonction arithmétique telle que m divise F_n si et seulement m divise n.

Vidéo 7 : Toute petite vidéo que je n'ai pas pu intégrer dans la précédente... On récolte ce que l'on a semé dans la vidéo Arithmétique 6 : on donne tous les nombres n tels que F_n se termine par exactement k zéros dans son écriture décimale. On rappelle que l'on a construit une fonction telle que m divise F_n si et seulement m divise n. Pour connaître m, il suffit donc de connaître p^k pour tout p de la décomposition en facteurs premiers de m. Et ceci est donné par une récurrence qui différencie les pas p =3 et $p = 2$.

Vidéo 8 : On présente ici l'équation de Pell-Fermat. Un résultat dit que, si d est un entier positif non carré, alors l'ensemble des solutions positives de l'équation diophantienne $x^2 - dy^2 = 1$ a une structure de groupe isomorphe à $\mathbb{Z}$. On montre ici, que cet ensemble est soit trivial, soit isomorphe à $\mathbb{Z}$.

Vidéo 9 : Un peu parce que l'on veut avoir le dernier mot avec l'équation de Pell-Fermat $x^2 - dy^2 = 1$, un peu pour la culture générale, mais aussi, pour la beauté de la chose, on va donner un mini-cours (en deux vidéos) sur les fractions continues. Ici, on montre que si x est un irrationnel, il possède une écriture sous forme de fraction continue et que celle-ci fournit une suite de rationnels qui tend vers x et, qu'elle approxime même x de façon remarquable (on parle d'approximation quadratique).

Vidéo 10 : Certaines équations diophantiennes comme l'équation de Pell-Fermat posent des problèmes d'approximation d'un réel par un rationnel. Plus particulièrement, l'équation de Pell-Fermat pose le problème d'approche d'un nombre quadratique par un rationnel. Il est alors temps de montrer ce joli théorème de Lagrange qui dit qu'un réel est quadratique si et seulement si sa décomposition en fraction continue est périodique à partir d'un certain rang.

Vidéo 11 : On finit par montrer, à l'aide des fractions continues, que l'équation de Pell-Fermat $x^2 - dy^2 = 1$ possède des solutions non triviales ! Attention à la fin, "faute de frappe" $324 + 325 = 649$ au lieu de 349 !

Vidéo 12 : Comme prétexte à présenter le petit lemme de Hensel, qui vient souvent

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

Courbes solutions de $X' = AX$ (2 vidéos) *(généralités, petits outils préliminaires en dimension n, changement de variable, dérivation sous le signe somme, classification des matrices modulo conjugaison et multiplication par un réel non nul, puis équations des courbes solution en dimension 2)*

Vidéo 1 : 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.

Vidéo 2 : On donne une autre approche pour l'allure des courbes dans $\mathbb{R}^2$ solutions de l'équation différentielle $X' = AX$. Cette approche passe par une classification plus grossière que celle des classes de similitude (on s'autorise à multiplier par un scalaire non nul).

Gymnastique des corps (8 vidéos)

Dans cette playlist, il ne s'agira pas de théorie des corps, mais juste d'un exposé de survol des différents types de corps sur lesquels on travaille dans le contexte de l'écrit, et pour chacun de ces types (caractéristique, finitude, ordre, algébriquement clos, les spécificités du corps des réels...), décrire les ouvertures que nous offre ce type et quels en sont les pièges. J'en parlerai dans le contexte 1) des algèbres de polynômes, 2) de la réduction 3) des formes quadratiques.

Vidéo 1 : On regarde attentivement les conséquences et les pièges qui se présentent selon si le corps sur lequel on travaille est fini ou non.

Vidéo 2 : Après avoir étudié les spécificités des corps infinis ou finis, on s'attaque au cas des corps de caractéristique zéro ou p.

Vidéo 3 : Ici, on regarde ce qui est possible ou pas, selon si l'on travaille (sur des polynômes, en réduction, ou formes quadratiques) sur un corps algébriquement clos ou non. On regarde ensuite les problèmes de caractéristiques 2 (ou pas).

Vidéo 4 : On regarde maintenant les spécificités du corps des réels, puis celui des complexes lorsque l'on travaille sur des polynômes ou sur la réduction.

Vidéo 5 : On continue sur ce volet de la pratique des corps à l'écrit de l'agrégation. On attaque ici une série de quatre vidéos sur les changements de corps. Sur cette vidéo un peu bavarde, il sera question de voir que chez les corps, les problèmes se font dans deux directions : la montée (on va chercher dans un corps plus grand des racines, des valeurs propres, des décompositions de polynômes...), et la descente (on a obtenu des 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.

Vidéo 6 : On attaque ici les problèmes de descente dans des cas pratiques. Tout d'abord, le pgcd de polynômes est invariant par changement de corps ; Puis, on voit que le rang d'une matrice possède également cette propriété d'invariance. C'est la porte ouverte à une première approche, sous forme d'exercices, de problème d'invariance par extension de corps invariants de classes de similitudes. On étudie le cas diagonalisable, nilpotent, et enfin la décomposition de Dunford.

Vidéo 7 : On pénètre ici dans le coeur du problème : montrer que deux matrices carrées sur un corps $\mathbb{K}$ sont semblables si et seulement si elles sont semblables sur une extension . Cette preuve se fait en deux temps : un premier temps où $\mathbb{K}$ contient toutes les valeurs propres et un second où il ne les contient pas. Dans ce dernier cas, on fait intervenir le corps de décomposition du polynôme caractéristique.

Vidéo 8 : On finit pour l'instant ce volet sur les extensions de corps et les théorèmes de descente. Autant ceux-ci fonctionnent trivialement pour la réduction, autant pour les formes quadratiques, on tombe sur des problèmes plus délicats, comme le prouve le théorème de Sylvester, qui est typiquement réel. On pourrait continuer longtemps sur ce sujet et peut-être le ferons-nous ultérieurement, par exemple, en parlant de semi-simplicité des endomorphismes, de la séparabilité, de théorèmes de descente en théorie des représentations... mais ces choses (passionnantes) sont un peu moins urgentes.

Matrices échelonnées (4 vidéos)

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

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

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

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

Espaces vectoriels agreg interne cours 1 cours 2 (12 vidéos)

Vidéo 1 : On commence un cycle d'algèbre linéaire qui figure au coeur du programme d'algèbre de l'agrégation interne. ici, il sera question de la définition des espaces vectoriels.

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

Vidéo 3 : Cette vidéo est dédiée au lemme d'échange qui permet de prouver que toutes les bases d'un espace vectoriel de dimension finie ont même cardinal.

Vidéo 4 : Dans cette vidéo 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.

Vidéo 5 : 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).

Vidéo 6 : La plupart des espaces vectoriels que l'on considère sont en fait 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.

Vidéo 7 : Voici 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.

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

Vidéo 9 : 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 critère de sommes directes.

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

Applications linéaires agreg interne cours 3 (6 vidéos)

Vidéo 1 : On définit les applications linéaires entre deux espaces vectoriel. Après quelques motivations, on en donne une forme générale lorsque les deux espaces sont les $\mathbb{K}$-espaces $\mathbb{K}^n$. On donne un exemple fondamental d'isomorphisme avec l'application qui, à un vecteur, associe son n-uplet de coordonnées dans une base fixée.

Vidéo 2 : 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.

Vidéo 3 : 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.

Vidéo 4 : 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.

Vidéo 5 : 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), que injectif est équivalent à surjectif. On donne deux contre-exemples en dimension finie.

Vidéo 6 : Une vidéo de synthèse pour tester notre compréhension du cours 3 et 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.

Arithmétique agrégation interne (8 vidéos)

Vidéo 1 : On introduit l'arithmétique. Vu l'abstraction de ce qui viendra par la suite, il est important 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 $\mathbb{Z}$, où le lemme de Gauss joue un rôle décisif.

Vidéo 2 : On continue sur le préambule motivant ! 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 donnait pas un aperçu suffisamment général de la situation.

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

Vidéo 4 : On attaque le cours d'arithmétique avec l'étude de l'anneau $\mathbb{Z}$. On suit

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

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

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

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

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

Dualité agreg interne (10 vidéos)

Vidéo 1 : On commence par parler par 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).

Vidéo 2 : On vient de voir les bases duales. Comment le changement de base duale dans E^* s'opère-t-il en fonction d'un changement de base fixé dans E ? On se rend compte que si l'on part d'une matrice de passage$P$ dans l'espace, alors on obtient une matrice de passage Q dans l'espace duale qui se trouve être, en générale, différente de P (Q est l'inverse de la transposée de P). Mais si l'on dualise une fois de plus la base duale, on obtient une matrice de passage à nouveau égale à P. Ceci permet de voir qu'il y a un isomorphisme indépendant d'une base choisie entre un espace E et son bidual.

Vidéo 3 : 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.

Vidéo 4 : 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.

Vidéo 5 : On étudie maintenant la dualité des sous-espaces vectoriel 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.

Vidéo 6 : 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.

Vidéo 7 : 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 $L(F^*, E^*)$.

Vidéo 8 : 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.

Vidéo 9 : On jongle ici avec le bidual pour montrer que la transposée est involutive. Mais si f est dans l'espace $L(E, F)$ des applications linéaires, la transposée de sa transposée est dans $L(E^{**}, F^{**})$. Que signifie donc l'égalité entre deux éléments qui n'appartiennent pas au même ensemble ? On va essayer d'expliquer cette subtilité. Ceux qui ne sont pas sensibles au concept alambiqué de bidual pourront se contenter de constater que la transposée possède une version matricielle beaucoup plus pratique.

Vidéo 10 : On fait le point sur des applications de la dualité dans le programme et les développements 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 agreg interne (6 vidéos)

Vidéo 1 : 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, mais en mettant l'accent sur le fait que ces liens dépendent de choix de bases. En même temps on définit les coordonnées (en colonne) des vecteurs dans une base, et en ligne des formes linéaires dans la base duale.

Vidéo 2 : 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.

Vidéo 3 : On définit deux involutions sur les matrices, tout d'abord la transposée et ensuite l'inversion des matrices (carrées inversibles !). On regarde à quoi correspond ces deux inversions dans le monde des applications linéaires (ou des endomorphismes).

Vidéo 4 : On présente ici les matrices de passage comme des matrices de l'application linéaire (en fait l'endomorphisme) identité avec pour base de départ la nouvelle base et pour base d'arrivée l'ancienne base. On montre que cette définition permet de retrouver très facilement toutes les formules sur les matrices de passage.

Vidéo 5 : On discute et on prouve ici l'incontournable théorème du rang qui dit que deux matrices sont équivalentes si et seulement si elles ont même rang.

Vidéo 6 : 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.

Epreuve Math Géné 2020 Agreg externe (12 vidéos) *(Suites arithmético-géométriques de matrices, Gram-Schmidt, décomposition QR, inégalité d'Hadamard, Cantor-Zassenhaus pour une méthode probabiliste visant à factoriser un polynome sur corps fini, inégalité de Minkowski pour trouver un vecteur dans un réseau, algorithme LLL)*

Vidéo 1 : En attendant les résultats (demain normalement)... On présente le problème de l'épreuve de mathématiques générales 2020 en mathématiques. On présente les différentes composantes du problème, ses qualités et ses défauts, autant dans son intérêt mathématique que dans ses capacités évaluatrices. Dans les prochaines vidéos (de 2 à 11), on rentrera dans les détails, sans toutefois se substituer à un corrigé.

Vidéo 2 : On présente les suites arithmético-géométriques dans$\mathbb{C}^n$. Ce sont des suites de vecteurs de la forme $X_{n+1} = AX_n + B$, où A est une matrice carrée et B un vecteur. Si 1 n'est pas dans le spectre de A, alors, c'est moralement une suite géométrique (à changement de variable près) et si A est la matrice identité, c'est une suite arithmétique. Dans les cas qui vont nous intéresser, c'est le lemme des noyaux qui fera le tri.

Vidéo 3 : On montre l'inégalité dite de la borne de Cauchy qui donne un bon majorant pour les module des racines d'un polynôme complexe P. On va en donner un corollaire qui donne une borne aux modules des coefficients des polynôme unitaires qui divisent P.

Vidéo 4 : Voici un lien classique (déjà discuté dans la vidéo 2 du "théorème du confinement") entre la méthode d'orthogonalisation de Gram-Schmidt, la décomposition QR, et l'inégalité d'Hadamard.

Vidéo 5 : Une factorisation d'un polynôme sur $\mathbb{Z}/p\mathbb{Z}$ peut être une bonne étape pour la factorisation sur $\mathbb{Z}$. On commence pour cela par factoriser le polynôme de $\mathbb{Z}/p\mathbb{Z}[X]$ en polynômes u_d, non nécessairement irréductibles, tels que leurs facteurs irréductibles soient de degré d. On montre dans cette vidéo comment effectuer cette première étape. Cette "stratification" par les polynômes u_d utilise le fait que $\mathbb{F}_p$ est un corps parfait, ou, plus simplement, que les polynômes $X^{p^d} - X$ n'ont pas de multiplicité quand on les décompose en facteurs de degré 1. Ensuite, on utilise un simple algorithme d'Euclide. On verra la

seconde étape dans la prochaine vidéo.

Vidéo 6 : On procède maintenant à la seconde étape de la factorisation d'un polynôme sur $\mathbb{Z}/p\mathbb{Z}$. La première étape nous ramène au cas où f se décompose en facteurs irréductibles de même degré d. On utilise une méthode probabiliste audacieuse due à Cantor et Zassenhaus : on choisit un polynôme g de degré strictement inférieur à celui de f. Si $\text{pgcd}(f, g)$ est non trivial, on casse le polynôme en deux et on continue sur ses morceaux. Si $\text{pgcd}(f, g) = 1$, on remplace g par $g^k - 1$ avec $k = (p^d - 1)/2$ et on voit que l'on toutes les chances d'obtenir $\text{pgcd}(f, g)$ est non trivial avec ce nouveau polynôme g.

Vidéo 7 : On présente ici succinctement le résultant. Il s'agit d'un déterminant qui permet de voir si deux polynômes sont ou non premiers entre eux. Lorsque les deux polynômes sont à coefficients entiers, on peut les réduire modulo p premier et voir, grâce à la réduction du résultant, si les deux polynômes réduits sont ou non premiers entre eux. Si p est assez grand par rapport aux coefficients des deux polynômes, l'inégalité d'Hadamard va montrer que les deux polynômes sont premiers entre eux dans $\mathbb{Z}$ si et seulement s'il sont premiers entre eux sur $\mathbb{Z}/p\mathbb{Z}$. C'est d'autant plus fort que la décomposition modulo p est plus simple à vérifier que dans $\mathbb{Z}$.

Vidéo 8 : On attaque l'articulation du problème d'agrégation MG 2020. Il s'agissait de comprendre un algorithme permettant de factoriser les polynômes dans $\mathbb{Z}[X]$. On commence par regarder la factorisation du polynôme donné modulo p assez grand par la méthode de Cantor-Zassenhaus (vue précédemment), puis les inégalités d'Hadamard sur le résultant permettent de remonter des informations de $\mathbb{Z}/pZ$ à $\mathbb{Z}$! On est amené à déterminer un vecteur de norme minimale dans un réseau.

Vidéo 9 : On a vu comment passer d'un problème de factorisation dans $\mathbb{Z}[X]$ à un problème de recherche d'un vecteur de norme minimale dans un réseau de $\mathbb{R}^n$. Dans cette vidéo on donne une borne min et une borne max pour ce plus petit vecteur, bornes qui s'expriment en fonction de la norme des vecteurs de la base orthonormalisée (par Gram-Schmidt) d'une base fixée du réseau. La borne min va utiliser encore une fois la décomposition QR et la borne max l'inégalité de Minkowski dans les réseaux.

Vidéo 10 : Une preuve simple de l'inégalité de Minkowski qui majore le plus petit vecteur d'un réseau.

Vidéo 11 : On expose très brièvement un algorithme qui permet de transformer une base d'un réseau de $\mathbb{R}^n$, en une base du même réseau permettant d'obtenir une base d'orthogonalisation à la Gram-Schmidt dont les vecteurs ne décroissent pas trop rapidement en norme. Cet algorithme a été motivé dans la vidéo 9 lorsque l'on voulait déterminer, en un temps polynomial en n, un vecteur de norme assez petite dans un réseau.

Déterminant (8 vidéos) *(forme n-linéaire alternée, unicité existence, multiplicativité, conséquences, mineurs et caractérisation du rang, formule de l'inverse par la comatrice, forme volume, développement de Laplace et formule de Binet)*

Vidéo 1 : On va parler de déterminants dans une série de vidéos. 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.

Vidéo 2 : On prouve et on illustre le théorème principal d'existence et d'unicité du déterminant.

Vidéo 3 : On a montré que l'ensemble des applications de $M_n(\mathbb{K})$ dans $\mathbb{K}$ 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.

Vidéo 4 : On observe dans cette vidéo les conséquence 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, 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 vidéo.

Vidéo 5 : On attaque la preuve de la formule explicite de l'inverse d'une matrice (inversible). On étudie ensuite les systèmes de Cramer.

Vidéo 6 : 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 égale à la taille maximale d'un mineur non nul. On illustre ensuite 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.

Vidéo 7 : Une petite vidéo presque simpliste sur le déterminant comme forme volume.

Vidéo 8 : 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.

Le groupe S_4 par Alain Debreil et Rached Mneimné (5 vidéos so far)

Vidéo 1 : Lecture d'été du joli livre d'Alain Debreil et Rached Mneimné chez Calvage et Mounet. Un livre qui ouvre toutes les fenêtres du groupe S_4 sur divers domaines des mathématiques. Dix-sept chapitres, et autant de notes fleuries qui embaumeront cette fin d'été.

Vidéo 2 : On feuillette ici le livre des métamorphoses du groupe symétrique S_4.

Vidéo 3 : On continue à feuilleter chapitre par chapitre les pages du livre d'Alain Debreil et Rached Mneimné sur les nombreux avatars du groupe S_4 en géométrie affine, euclidienne, avec les polytopes, les graphes de Cayley, les treillis d'extensions de corps et enfin la géométrie projective. Ces deux derniers méritent un traitement à part qui figurera dans des vidéos prochaines.

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

Vidéo 5 : On prouve le résultat annoncé sur le nombre de décomposition dans S_n en types donnés. Cela demande de la théorie des caractères (lemme de Schur et surtout l'utilisation classique de la représentation régulière comme fonction caractéristique de l'élément neutre).

Ampoules et interrupteurs formes quadratiques en caractéritique 2 (5 vidéos)

Vidéo 1 : On va introduire deux problèmes autour d'ampoules et interrupteurs sous forme de quizz (niveau minimal L3 pour le premier et M1 pour le second). Dans les deux cas, la solution doit son salut à l'intervention de formes quadratiques sur $\mathbb{F}_2$. Ou plutôt, de formes bilinéaires symétriques sur l'espace $\mathbb{F}_{2^n}$, ce qui, en caractéristique 2, est assez différent.

Vidéo 2 : On introduit deux problèmes autour d'ampoules et interrupteurs sous forme de quizz (niveau minimal L3 pour le premier et M1 pour le second). Dans les deux cas, la solution doit son salut à l'intervention de formes quadratiques sur $\mathbb{F}_2$. Ou plutôt, de formes bilinéaires symétriques sur l'espace $\mathbb{F}_{2^n}$, ce qui, en caractéristique 2, est assez différent.

Vidéo 3 : On introduit deux problèmes autour d'ampoules et interrupteurs sous forme de quizz (niveau minimal L3 pour le premier et M1 pour le second). Dans les deux cas, la solution doit son salut à l'intervention de formes quadratiques sur $\mathrm{F}_2.Ouplutt, deformesbilinairessymtr$

Vidéo 4 : On introduit deux problèmes autour d'ampoules et interrupteurs sous forme de quizz (niveau minimal L3 pour le premier et M1 pour le second). Dans les deux cas, la

solution doit son salut à l'intervention de formes quadratiques sur F_2.$Ouplutt, de formes bilinaires symtr$

Vidéo 5 : On compte maintenant le nombre de solutions au problème des rampes de spots et on se ramène à dénombrer le groupe orthogonal $\mathrm{O}_n(F_2)$, $ce quise fait par r currence$.

Réduction – polynômes d'endomorphisme (7 vidéos)

Vidéo 1 : On commence un nouveau cours d'agrégation interne sur la réduction. Tout d'abord avec une partie motivation, 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, histoire de lancer le programme.

Vidéo 2 : On commence par définir les polynômes d'un endomorphisme u d'un espace vectoriel E. Ce ci est défini comme un morphisme d'algèbre allant de l'agébre de polynômes $\mathbb{K}[X]$ vers l'algèbre des endomorphismes de E. Ce morphisme définit, d'une part, l'algèbre des polynômes de l'endomorphisme u, et d'autre part, le polynôme minimal de u, vu comme générateur de l'idéal noyau.

Vidéo 3 : On attaque la preuve du lemme des noyaux, qui peut être vu comme un avatar de l'identité de Bezout (et finalement l'arithmétique des polynômes) dans la géométrie de l'espace E "muni de l'endomorphisme u".

Vidéo 4 : En mathématiques, on est toujours confronté au choix de la théorie et de la pratique. Le polynôme minimal est un polynôme annulateur (d'un endomorphisme u), plutôt du côté de la théorie. En revanche, le polynôme caractéristique est un polynôme plus facilement calculable par sa définition et également annulateur par Cayley-Hamilton. Ses racines sont les valeurs propres de l'endomorphisme u.

Vidéo 5 : On prouve ici le théorème de Cayley-Hamilton par les matrices compagnon.

Vidéo 6 : On fait le point sur les propriétés du polynôme caractéristique. Degré, indépendance du corps, divisibilité par le polynôme minimal mu et divise mu^n.

Vidéo 7 : On a montré que le polynôme caractéristique était "coincé" entre le polynôme minimal et une puissance (égale à la dimension de l'espace) du polynôme minimal. On en donne une preuve alternative instructive lorsque le corps est le corps des complexes (ou un corps algébriquement clos). On en déduit ensuite le polynôme minimal et caractéristique d'un endomorphisme restreint aux sous-espaces caractéristiques.

Polynômes (7 vidéos)

Vidéo 1 : On définit ici l'anneau des polynômes $A[X]$ (ou $\mathbb{K}[X]$) sur un anneau intègre unitaire A (ou sur un corps $\mathbb{K}$). On en donne une "base", on étudie les propriétés du degré, l'injection naturelle de A dans $A[X]$, et enfin, cette spécificité de l'anneau de polynôme : le morphisme d'évaluation.

Vidéo 2 : On étudie l'arithmétique de l'anneau $K[X]$. Tout commence avec la notion de degré qui permet de définir un division euclidienne. A partir de là tout s'enchaîne : l'anneau $K[X]$ est principal, et donc factoriel. On étudie ensuite les anneaux quotient de $\mathbb{K}[X]$ par un idéal (forcément principal) et on montre que si P est non nul, $\mathbb{K}[X]/(P)$ est un $\mathbb{K}$-espace de dimension $\deg(P)$.

Vidéo 3 : On introduit le problème de 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 $(X - a_i)$.

Vidéo 4 : On étudie la $\mathbb{K}$-algèbre des fonctions polynômes en prenant soin de la distinguer de la $\mathbb{K}$-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 $\mathbb{K}$ est infini, alors le morphisme est iso et on peut confondre les deux algèbres. On fait l'étude lorsque le corps $\mathbb{K}$ est fini où l'on exhibe le noyau du morphisme.

Vidéo 5 : 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 iso 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.

Vidéo 6 : On commence ici à s'intéresser aux relations coefficients/racines. On introduit 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 : tout polynôme symétrique de $\mathbb{Z}[X_1, ..., X_n]$ 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 dans une prochaine vidéo.

Vidéo 7 : On prouve 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.

Diagonalisation