Autocorrection de l'épreuve MG 2020 (Agreg externe)

Pour avoir l'épreuve sous les yeux, cliquez ici.

Exercice 1.

1. • Résolution du système $\boxed{1}$
   • Réciproque (vérification) $\boxed{0,5}$
2. • déterminant nul $\boxed{0,5}$
   • formule du rang $\boxed{0,5}$
3. • Une matrice est trigonalisable sur $\mathbb{C}$ et les valeurs propres (avec multiplicité algébrique) sont sur la diagonale $\boxed{1}$
   • la trace est un invariant de similitude $\boxed{0,5}$
   • la trace est somme des valeurs propres (avec multiplicité algébrique) $\boxed{0,5}$
   • comme $m_g(0) < m_a(0)$, c'est non diagonalisable. $\boxed{1}$

Exercice 2.

1. • Si (contraposée) $A - \lambda \mathrm{Id}$ est non inversible, λ est valeur propre. $\boxed{0,5}$
   • un vecteur propre v pour λ est alors non nul et donc $\max_i |v_i| > 0$. $\boxed{1,5}$
   • inégalité $|a_{ii} - \lambda| \leq \sum_{i \neq j} |a_{ij}|$ $\boxed{1}$
2. • Rappel que $\chi_{A_f} = f$. $\boxed{0,5}$
   • $f(\lambda) = 0$ implique λ v.p. de A_f et conclusion. $\boxed{1}$
3. • on vérifie l'inégalité pour $i = 1$ $\boxed{0,5}$
   • on vérifie l'inégalité pour $1 < i < d$ $\boxed{1}$
   • on vérifie l'inégalité pour $i = d$ $\boxed{0,5}$
   • En déduire l'inégalité (sans remarquer qu'il faut prendre le max sur $1 \leq i \leq d$, et non pas $d - 1$). $\boxed{0,5}$
   • En remarquant qu'il faut prendre le max sur $1 \leq i \leq d$. $\boxed{1}$

4. • Calculer g_k à l'aide des relations coefficients racines (en disant que g est unitaire) $\boxed{1,5}$
   • Etablir l'inégalité $\boxed{2,5}$

Exercice 3.

1. (a) • Inclusion $\text{Vect}(b_1, \cdots, b_i) \subset \text{Vect}(b_1^*, \cdots, b_i^*)$ $\boxed{0,5}$
   • inclusion inverse (par la dimension). $\boxed{1}$
   • En déduire b_i^* non nul. $\boxed{0,5}$

   (b) • Mise en place de la récurrence (initialisation-hérédité) $\boxed{1}$
   • utilisation de $b_i^* \neq 0$ pour diviser par (b_i^*, b_i^*). $\boxed{1}$

   (c) • Mise en place d'une récurrence sur i, avec $j < i$. $\boxed{1}$
   • calcul de (b_i^*, b_j^*). $\boxed{1}$
2. On pose $E := \langle b_1, \cdots, b_d \rangle = \langle b_1^*, \cdots, b_d^* \rangle$.
   • la matrice ${}^tBB$ est la matrice $(b_i, b_j)_{1 \leq i,j \leq d}$ qui est la matrice de $(\ ,\ )$ restreinte à $E \times E$ dans la base $\underline{b}$ de E. $\boxed{1}$
   • la matrice $D := \text{diag}\left((b_i^*, b_i^*)\right)$ est la matrice de $(\ ,\ )$ restreinte à $E \times E$ dans la base $\underline{b}^*$ de E. $\boxed{1}$
   • la matrice de passage P de $\underline{b}^*$ à $\underline{b}$ est triangulaire supérieure avec des 1 sur la diagonale. $\boxed{1}$
   • ${}^tBB = {}^tPDP$ par la formule de changement de bases et on conclut avec le déterminant. $\boxed{1}$
3. • $d = n$ et donc $\det(B)$ et $\det({}^tB)$ ont un sens (les matrices sont carrées) et sont égaux. $\boxed{1}$
   • $|\det(B)| = \prod_i ||b_i^*||_2$. $\boxed{1}$
   • Pythagore pour montrer que $||b_i^*||_2 \leq ||b_i||_2$ et on conclut. $\boxed{1,5}$

Exercice 4.

1. • P_k est unitaire, donc la division euclidienne de P_n par P_k dans $\mathbb{Q}[t]$ donne des quotients et restes dans $\mathbb{Z}[t]$. $\boxed{1,5}$
   • $p^r - 1$ divise $p^{qr} - 1$ dans $\mathbb{Z}$. $\boxed{1}$
   • $t^{p^r-1} - 1$ divise $t^{p^k(p^{qr}-1)} - 1$ dans $\mathbb{Z}[t]$, donc il divise $t^{p^k}(t^{p^k(p^{qr}-1)} - 1)$. Et donc P_r divise $P_n - P_k$. $\boxed{1,5}$
   • Unicité de la division euclidienne. $\boxed{1}$
2. • Décrire brièvement l'algorithme d'Euclide pour le calcul d'un pgcd. $\boxed{1}$
   • 1) prouve que l'algorithme d'Euclide sur (n, r) fournit directement l'algorithme d'Euclide sur (P_n, P_r). $\boxed{1}$
3. • $\mathbb{Z}/p\mathbb{Z}[t]/(f)$ est un anneau. $\boxed{0,5}$
   • $\mathbb{Z}/p\mathbb{Z}[t]/(f)$ est un corps par l'identité de Bezout à f irréductible. $\boxed{1}$
   • la dimension de $\mathbb{Z}/p\mathbb{Z}[t]/(f)$ sur $\mathbb{Z}/p\mathbb{Z}$ est égale au degré de f, c'est-à-dire r, avec une petite preuve rapide. $\boxed{1}$

• on conclut la cardinalité de $\mathbb{Z}/p\mathbb{Z}[t]/(f)$, c'est-à-dire p^r. $\boxed{0,5}$

• on énonce l'unicité à isomorphisme près d'un corps de cardinal p^r. $\boxed{0,5}$

• On rappelle que $\mathbb{F}_{p^r}$ est constitué d'éléments tels que $x^{p^r} - x = 0$. $\boxed{0,5}$

• P_r s'annule sur $\mathbb{Z}/p\mathbb{Z}[t]/(f)$. $\boxed{1}$

• f divise P_r. $\boxed{0,5}$

4. On note φ irréductible sur $\mathbb{F}_p$ de degré divisant n.

• D'après la question 3, φ divise $\pi_p(P_k)$, avec $k = \deg(\varphi)$. $\boxed{1}$

• Avec k comme ci-dessus, P_k divise P_n dans $\mathbb{Z}[t]$ par la question 1. $\boxed{1}$

• π_p est un morphisme de l'anneau $\mathbb{Z}[t]$ sur l'anneau $\mathbb{F}_p[t]$. Donc, $\pi_p(P_k)$ divise $\pi_p(P_n)$ dans $\mathbb{F}_p[t]$. $\boxed{0,5}$

• le ppcm des φ est égal à $\prod_\varphi$ car ils sont irréductibles distincts, donc premiers entre eux. $\boxed{0,5}$

• Q, c'est-à-dire $\prod \varphi$ divise $\pi_p(P_n)$. $\boxed{1}$

Partie I.

1. (a) • $\mathcal{E}$ est vecteur propre. $\boxed{0,5}$

• H est stable (par exemple, c'est l'orthogonal d'une droite stable par une matrice symétrique). $\boxed{1}$

(b) • Se ramener à montrer que $x_k^2 + 2x_kx_{k+1} + x_{k+1}^2 \leq 2x_k^2 + 2x_{k+1}^2$ et le montrer. $\boxed{1}$

• Cas d'égalité $x_{k+1} = x_k$. $\boxed{1}$

2. • $\mathcal{E}$ est vecteur propre de A. $\boxed{0,5}$

• H est stable par A. $\boxed{0,5}$

3. • Si x n'est pas sur la droite $\mathbb{R}\mathcal{E}$, alors $x_k \neq x_{k+1}$ pour un k. Puis, on applique 1b) pour l'inégalité $||Ax||_2 < ||x||_2$. $\boxed{1,5}$

• Comme $\mathbb{R}\mathcal{E}$ et H sont des supplémentaires stables par A par 2), le spectre de A est la réunion du spectre de l'induit sur $\mathbb{R}\mathcal{E}$ et de l'induit sur H. Le spectre sur H est dans le disque ouvert. $\boxed{1,5}$

• Le spectre sur H est dans le disque ouvert unité par l'inégalité $||Ax||_2 < ||x||_2$, valable pour x non nul dans H. $\boxed{1}$

• Si jamais, au cours de la rédaction, vous avez écrit "si $x \notin \mathbb{R}\mathcal{E}$, alors $x \in H$", Jean-Michel Blanquer vous tondra en place publique tout en chantant "Pour que tu m'aimes encore" de Celine Dion et Cédric Villani viendra vous tatouer sur le crâne les axiomes de base des espaces vectoriels sur l'air de "The final countdown", mais en se contentant de faire "tantantaaantaaaan" parce qu'il ne connaît pas les paroles.

4. • La norme deux de $A_H^k \cdot x$ tend vers 0. $\boxed{1}$

• Les normes sont équivalentes et on choisit la norme de A_H^k est égale au max sur une sphère (pour une norme de votre choix). On voit alors que la norme de A_H^k tend vers 0 d'après ce qui précède. $\boxed{1,5}$

5. • on montre que $(A^k - \Pi).x$ tend vers 0. $\boxed{1}$
   • On conclut comme dans la question précédente avec une norme choisie. $\boxed{1}$
6. • $A_H - \mathrm{Id}_H$ est inversible par 3) et on conclut. $\boxed{1}$
   • on utilise 2) pour scinder $X = AX + G$ en deux égalités $X_{\mathcal{E}} = AX_{\mathcal{E}}$ et $X_H = A_H X_H + G$, avec $X = X_{\mathcal{E}} + X_H$ la décomposition de X sur $\mathbb{R}\mathcal{E} \oplus H$. $\boxed{1,5}$
   • On conclut que $X \in \mathbb{R}\mathcal{E} + Z$. $\boxed{1}$
7. • Premier changement de variables $X_\ell = \Pi(X_0) + Y_\ell$. $\boxed{1}$
   • Second changement de variables $Y_\ell = Z + Z_\ell$. $\boxed{1}$
   • $Z_{\ell+1} = A_H Z_\ell$ et on conclut. $\boxed{1}$

Cliquez ici: la playlist de 11 vidéos pour aller plus loin sur le sujet 2020

Epreuve Math Géné 2020 Agreg externe (11 vidéos) *(Suites arithmético-géométriques de matrices, Gram-Schmidt, décomposition QR, inégalité d'Hadamard, Cantor-Zassenhaus pour une méthode probabiliste visant à factoriser un polynôme 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 modules 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.