Liste non exhaustive de classiques

Tome II : Algèbre / Probabilités

Une compilation d'exercice mathématiques
pour étudiants de classe préparatoire MP, PSI et PC

Auteur : Marconot Lorenzo , Esteve Arthur

Collection Prépas – Mathématiques

lycée Dumont D'Urville

A M. Garcin et M. Teyssier,
à Tan, la légende,
à Arsinoé, Félix et Célian qui nous ont inspiré,
et aux 5/2 de la promo 2024-2025.
"La prépa, c'est du sang, des larmes et de la sueur".

Avant Propos

Salut à toi jeune CPGEiste, alors si aujourd'hui je me permets de te contacter, c'est pour une raison très simple : savais-tu que 95 % des étudiants en prépa ne savent pas comment aborder un problème ? Alors, est-ce que tu veux en faire partie ? Il faut que tu te poses les bonnes questions. Est-ce que tu préfères faire pitié ou commencer très rapidement à accumuler du savoir avec moi grâce à ton téléphone et pouvoir faire partie de l'élite ? Moi, je pense que la question, elle est vite répondue.

Bon, en vrai sans déconner, Arthur et moi-même sommes passés par-là, on a fait 3 ans de classe préparatoire au lycée Dumont d'Urville, donc on connaît très bien la prépa et ses enjeux. On a voulu transmettre un morceau de ce que l'on pense qui vous sera utile, à l'instar de nos 5/2 (s/o Arsinoé Payet, Félix Gauci et Célian Rosello) qui ont écrit un formulaire en Chimie et en SI (que je ne saurais trop vous conseiller de lire avant chaque DS pour revoir les formules à connaître). On souhaite que soit transmis un héritage au sein de Dumont pour que chaque année, les prédécesseurs aident les suivants.

Déjà, à qui servent-ils ? Il est utile à tout étudiant peu importe son niveau ou son ambition. Dans cet ouvrage, on a essayé de compiler tous les exercices classiques (vus en colle, en DS ou en TD) que l'on a trouvés pertinents, car ils sont soit omniprésents aux concours, soit demandant un raisonnement qu'il est impératif d'avoir vu pour acquérir des réflexes très utiles si l'on est bloqué. Il est vrai que ce recueil d'exercices contient énormément d'exercices difficiles, mais il ne faut pas avoir peur : il y a énormément d'exercices abordables et que vous devez impérativement faire et puis, pour réussir en prépa, il faut « avoir les dents qui rayent le parquet », faut vouloir tout déchirer pour obtenir ce que l'on veut et c'est à cela que servent ces ouvrages : vous proposer une liste d'exercices qu'il faut voir (et revoir autant de fois que nécessaire) avant les concours. Ces ouvrages sont également destinés aux étudiants ne souhaitant pas faire d'études d'ingénieur et qui souhaitent aller en licence. Ils permettent d'avoir toutes les bases nécessaires pour appréhender en toute confiance les chapitres de la L3.

Bon, cet ouvrage est uniquement là en complément de cours : il faut d'abord assimiler le cours avec le prof pour pouvoir s'en sortir en prépa, donc on privilégie les exos du TD. On a créé ce recueil pour que les théorèmes ou résultats classiques soient recensés au même endroit.

P.-S. : On essaie de compléter au fur et à mesure les corrections des deux livres, cela demande un temps de dingue mais on promet de proposer un maximum de corrigés avant les concours.

P.-P.-S. : Ce message est destiné à tous les futurs 5/2, je souhaiterais que pendant votre temps de révision, vous envisagiez de perpétuer l'héritage pour que d'ici quelques années Dumont d'Urville soit au sommet. Je ne vous demande pas de faire un aussi gros projet, mais cela serait vraiment super de pouvoir aider les futurs élèves à relever le défi qu'est la prépa en toute confiance.

Légende et notations

Un exercice est affilié d'un certain nombre d'étoiles ★ relativement à sa difficulté :

- ★ Démonstration ou application directe du cours (le plus souvent E3A, CCINP) ;
- ★★ Application du cours/de méthodes usuelles (le plus souvent CCINP, Mines-Télécom) ;
- ★★★ Application du cours/de méthodes usuelles (le plus souvent Centrale, Mines-Ponts) ;
- ★★★★ Exercice exotique/peu ou pas guidé (Centrale, Mines-Pont, X-ENS) ;
- ★★★★★ Exercice exotique/peu ou pas guidé (le plus souvent X-ENS).

Ces étoiles suivent un code couleur indicatif du concours auquel l'exercice aurait le plus de chance d'être posé, à l'écrit ou à l'oral :

- Aucun concours spécifique ★
- E3A/CCINP ★
- Mines-Télécom ★
- Mines-Ponts/Centrale ★
- X-ENS ★

Pour des exercices considérés comme des "classiques" qui tombent régulièrement, le titre de l'exercice sera souligné.
Par exemple Série harmonique : ★★★ indique que l'exercice nommé "Série harmonique" est un immanquable de tous les candidats qui se préparent à E3A/CCINP.
Enfin, un exercice qui utilise ou traite des notions hors du programme (de MP) sera suivi d'un label (HP).
Dernière chose, il a été mis en place un système d'hyperlien permettant une navigation rapide et simple, ainsi toute la table de matière est cliquable et depuis un lien direct entre l'énoncé et sa correction l'est également à l'aide des balises [Enoncé] ou [Corrigé]

Table des matières

I Algèbre linéaire

Dans toute cette section n désigne un entier naturel non nul.

I.1 Extension de corps ★★ (HP)

[Corrigé]

1. Donner un exemple de sous-espace vectoriel réel d'un $\mathbb{C}$-espace vectoriel qui n'est pas un $\mathbb{C}$-espace vectoriel.
2. Soit V un $\mathbb{C}$-espace vectoriel de dimension p.
   Démontrer que V est un $\mathbb{R}$-espace vectoriel de dimension $2p$.
3. On considère un corps commutatif $(\mathbb{M}, +, \times)$ et $\mathbb{K} \subset \mathbb{L}$ deux sous-corps de $\mathbb{M}$.
   Démontrer l'équivalence des deux assertions :
   (i) $\mathbb{M}$ est un $\mathbb{K}$-espace vectoriel de dimension finie m ;
   (ii) $\mathbb{M}$ est un $\mathbb{L}$-espace vectoriel de dimension finie k et $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel de dimension finie p.

   Montrer que dans ces conditions $m = kp$. (relation de multiplicativité des degrés)

I.2 Passage du complexe au réel

[Corrigé]
Soient V un $\mathbb{C}$-espace vectoriel de dimension n et $v \in \mathcal{L}(V)$. On note W l'espace V munit de sa structure naturelle de $\mathbb{R}$-espace vectoriel de dimension $2n$ et on note $u \in \mathcal{L}(W)$ l'endomorphisme de W défini comme étant égal à v.
Montrer que $\det(w) = |\det(v)|^2$.

I.3 Dimension de $\mathbb{R}$ en tant que $\mathbb{Q}$-espace vectoriel ★★ (HP)

[Corrigé]

1. Montrer que $\mathbb{R}$ est un $\mathbb{Q}$-espace vectoriel.
2. Montrer que si $p_1, \dots, p_n$ sont des nombres premiers distincts alors la famille $(\ln(p_1), \dots, \ln(p_n))$ est $\mathbb{Q}$-libre.
3. Quelle est la dimension de $\mathbb{R}$ en tant que $\mathbb{Q}$-espace vectoriel ?

I.4 Indépendance des fonctions

[Corrigé]

Soient X un ensemble et $(f_1, \dots, f_n)$ une famille libre de $\mathbb{C}^X$.
Montrer qu'il existe $x_1, \dots, x_n \in X$ tels que ma matrice $(f_i(x_j))_{1 \leq i,j \leq n}$ soit inversible.

I.5 L'ordre a son importance

[Corrigé]
Soit $M \in \mathcal{M}_n(\mathbb{R})$.
Montrer l'équivalence entre les affirmations :

— $\forall A, B \in \mathcal{M}_n(\mathbb{R})$, $\mathrm{Tr}(MAB) = \mathrm{Tr}(MBA)$

— M est une homothétie.

I.6 Centre de $\mathcal{M}_n(\mathbb{K})$ ★★

[Corrigé]
Déterminer le centre de $\mathcal{M}_n(\mathbb{K})$: $Z = \{A \in \mathcal{M}_n(\mathbb{K}),\ \forall B \in \mathcal{M}_n(\mathbb{K}),\ AB = BA\}$.

I.7 Racine carrée de la dérivation ★★★

[Corrigé]
On note $E = \mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$ et $\Delta : \left\{ \begin{array}{ccc} E & \longrightarrow & E \\ f & \longmapsto & f' \end{array} \right.$.
Existe-t-il un endomorphisme $\delta \in \mathcal{L}(E)$ tel que $\delta^2 = \Delta$?

I.8 Produit de matrices nilpotentes ★★★★★

[Corrigé]
Soient $N_1, \dots, N_n \in \mathcal{M}_n(\mathbb{K})$ des matrices nilpotentes qui commutent toutes entre elles.
Montrer que $\prod_{i=1}^{n} N_i = 0$.

I.9 Suites périodiques ★★★★

[Corrigé]
On note E le sous-ensemble de $\mathbb{C}^{\mathbb{N}}$ composé des suites périodiques.
Montrer que E est un espace vectoriel et en déterminer une base.

I.10 Dimension du commutant (1)

[Corrigé]
Soit u un endomorphisme d'un $\mathbb{C}$-espace vectoriel E de dimension finie.
On pose $f_u : \left\{ \begin{array}{ccc} \mathcal{L}(E) & \longrightarrow & \mathcal{L}(E) \\ v & \longmapsto & u \circ v - v \circ u \end{array} \right.$ et on note $\mathcal{C}(u) = \{v \in \mathcal{L}(E),\ u \circ v = v \circ u\}$.

1. Montrer que $\mathcal{C}(u)$ est un sous-espace vectoriel de $\mathcal{L}(E)$.
2. Montrer que $\dim \mathcal{C}(u) \geq \dim E$.

I.11 Etude de la comatrice ★★★

[Corrigé]

1. Calculer $\mathrm{Com}(J_r)$ pour $0 \leq r \leq n$.
2. Démontrer que $\forall (A, B) \in \mathcal{M}_n(\mathbb{K})^2,\ \mathrm{Com}(AB) = \mathrm{Com}(A)\,\mathrm{Com}(B)$.
3. En déduire le rang de la comatrice de A en fonction du rang de A.
4. Soit $\varphi : \left\{ \begin{array}{ccc} \mathcal{M}_n(\mathbb{K}) & \longrightarrow & \mathcal{M}_n(\mathbb{K}) \\ A & \longmapsto & \mathrm{Com}(A) \end{array} \right.$.
   φ est-elle injective ? Surjective ?
   Déterminer $\mathrm{Im}(\varphi)$ dans le cas $\mathbb{K} = \mathbb{C}$.

I.12 Lemme de Schur ★★

[Corrigé]
Soit $\mathbb{K}$ un corps. Soit u un endomorphisme de E un $\mathbb{K}$-espace vectoriel tel que pour tout $x \in E$, $(x, u(x))$ est une famille liée.
Montrer que u est une homothétie vectorielle.

I.13 Espaces engendrés par les matrices inversibles et orthogonales ★★★

[Corrigé]

1. Déterminer $\mathrm{Vect}(\mathrm{GL}_n(\mathbb{K}))$.
2. Déterminer $\mathrm{Vect}(\mathcal{O}_n(\mathbb{R}))$.

I.14 Espace engendré par les matrices nilpotentes ★★★

[Corrigé]
Montrer que l'espace vectoriel engendré par les matrice nilpotentes est l'ensemble des matrices de trace nulle.

I.15 Transmission d'information ★★★

[Corrigé]
Soient $A, B \in \mathcal{M}_n(\mathbb{K})$ telles que $\forall X \in \mathcal{M}_n(\mathbb{K}),\ AXB = 0$.
Montrer que $A = 0$ ou $B = 0$.

I.16 Noyau et Image supplémentaires ★★

[Corrigé]
Soit f un endomorphisme d'un espace vectoriel E.
Montrer que les trois propositions sont équivalentes :

— $E = \mathrm{Im}(f) \oplus \mathrm{Ker}(f)$
— $\mathrm{Im}(f^2) = \mathrm{Im}(f)$
— $\mathrm{Ker}(f^2) = \mathrm{Ker}(f)$

I.17 Théorème de Maschke

[Corrigé]

Soit E un espace vectoriel de dimension finie et soit G un sous-groupe fini de $GL(E)$ de cardinal n.

1. Etudions un objet mathématique courant dans l'étude des groupes dans le but de comprendre la méthode utilisé pour la suite.
   (a) Montrer que si p est un projecteur, alors $\text{rg}(p) = \text{Tr}(p)$.
   (b) Soit $h \in G$. Montrer que $\varphi_h : g \in G \to h \circ g$ est une permutation de G.
2. On pose $p = \dfrac{1}{n} \displaystyle\sum_{g \in G} g$.
   (a) Montrer que p est un projecteur.
   (b) Montrer que
   $$\dim\left(\bigcap_{g \in G} \text{Ker}(g - Id_E)\right) = \frac{1}{n} \sum_{g \in G} \text{Tr}(g)$$
3. Soit F un sous-espace vectoriel de E stable par tous les éléments de G et H un supplémentaire de F. On note q le projecteur sur F parallèlement à H.
   Montrer qu'il existe un supplémentaire de F stable par tous les éléments de G.
   Indication : on étudiera $\dfrac{1}{n} \displaystyle\sum_{g \in G} g^{-1} \circ q \circ g$

II Réduction géométrique

Dans toute cette section n désigne un entier supérieur ou égal à 1.

II.1 Matrices de rang 1

[Corrigé]

II.1.1 Réduction des matrices de rang 1 ★

1. Soit $M \in \mathcal{M}_n(\mathbb{K})$. Montrer que :
$$\mathrm{rg}(M) = 1 \iff \exists (U, V) \in (\mathcal{M}_{n,1}(\mathbb{K}))^2 \text{ non nulles tel que } M = UV^\top$$
2. Soit $M \in \mathcal{M}_n(\mathbb{K})$ une matrice de rang 1, montrer que $M^2 = \mathrm{Tr}(M)M$.
3. Donner une condition nécessaire et suffisante pour qu'une matrice de rang 1 soit diagonalisable.
4. Application : Résoudre l'équation $A^3 = \begin{pmatrix} 1 & -2 & 1 \\ 1 & -2 & 1 \\ 1 & -2 & 1 \end{pmatrix}$.

II.1.2 Diagonalisabilité d'une matrice ★★★

Soient $a_1 \leq \cdots \leq a_n$ et $b_1 > \cdots > b_n > 0$ des réels. On considère la matrice
$$M = \begin{pmatrix} a_1 & b_2 & \dots & b_{n-1} & b_n \\ b_1 & a_2 & \ddots & \vdots & \vdots \\ \vdots & b_2 & \ddots & b_{n-1} & b_n \\ \vdots & \vdots & \ddots & a_{n-1} & b_n \\ b_1 & b_2 & \dots & b_{n-1} & a_n \end{pmatrix}$$

1. Exprimer χ_M en fonction des a_i et des b_i.
   On pourra utiliser le lemme du déterminant (cf. VIII-50 tome Analyse)
2. Démontrer à l'aide du TVI que M est diagonalisable dans $\mathbb{R}$.

II.2 Matrices réelles semblables ★★

[Corrigé]
Soient A et B deux matrices de $\mathcal{M}_n(\mathbb{R})$ semblables sur $\mathbb{C}$.
Montrer que A et B sont semblables sur $\mathbb{R}$.

II.3 Complément de Schur ★★

[Corrigé]
Soit $p, q \in \mathbb{N}^*$.
Soit $M = \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$ avec $A \in GL_p(\mathbb{K})$ et $D \in \mathcal{M}_q(\mathbb{K})$.
On pose $S = D - CA^{-1}B$.

1. Montrer que $\det(M) = \det(A)\det(S)$.
2. Montrer que $\mathrm{rg}(M) = \mathrm{rg}(A) + \mathrm{rg}(S)$.

II.4 Produit de Kronecker ★★

[Corrigé]
Pour $A, B \in \mathcal{M}_2(\mathbb{K})$ on note $A \otimes B = \left(\begin{array}{c|c} a_{11}B & a_{12}B \\ \hline a_{21}B & a_{22}B \end{array}\right)$.

1. Soit $(A, B, C, D) \in \mathcal{M}_2(\mathbb{K})^4$. Montrer que $(A \otimes B).(C \otimes D) = (AC) \otimes (BD)$
2. Calculer $\det(A \otimes I_2)$, $\det(I_2 \otimes B)$ et $\det(A \otimes B)$ en fonction de $\det A$ et $\det B$.
3. A quelle condition $A \otimes B$ est-elle inversible ? Quelle est alors son inverse ?
4. On suppose que A et B sont diagonalisables. Montrer que $A \otimes B$ est diagonalisable.

II.5 Disques de Gershgorin ★★

[Corrigé]

1. Soit $A \in \mathcal{M}_n(\mathbb{C})$. Pour $i \in [\![1; n]\!]$ on note $R_i = \sum_{j \neq i} |a_{ij}|$.
   Montrer que toute valeur propre de A appartient à au moins un des disques fermés de centre a_{ii} et de rayon R_i.

2. En déduire le lemme de Hadamard : Toute matrice à diagonale strictement dominante (i.e $\forall i \in [\![1;n]\!],\ |a_{ii}| > R_i$) est inversible.

II.6 Spectre de $u \circ v$ et $v \circ u$ ★

[Corrigé]
Soit u et v deux endomorphismes d'un $\mathbb{K}$-espace vectoriel de dimension finie. Montrer que $u \circ v$ et $v \circ u$ ont les mêmes valeurs propres.

II.7 Endomorphismes qui commutent ★★

[Corrigé]
Soient E un $\mathbb{C}$-espace vectoriel de dimension finie et $(u, v) \in \mathcal{L}(E)^2$.
Montrer que si u et v commutent, alors ils ont un vecteur propre commun.

II.8 Vecteur propre commun ★★★

[Corrigé]
Soient E un $\mathbb{C}$-espace vectoriel de dimension finie et $(u, v) \in \mathcal{L}(E)^2$.
Montrer que u et v ont un vecteur propre commun dans chacun des cas suivant :

1. $u \circ v = 0$.
2. $\exists a \in \mathbb{C},\ u \circ v = au$.
3. $\exists b \in \mathbb{C},\ u \circ v = bv$.
4. $u \circ v = \mathrm{Id}_E$.
5. $\exists (a, b) \in \mathbb{C}^2,\ u \circ v = au + bv$.

II.9 Eléments propres d'un endomorphisme (1) ★★

[Corrigé]
Soit $(E, \langle\ ,\ \rangle)$ un espace euclidien. On considère des vecteurs unitaires a et b formant une famille libre de E.
Réduire l'endomorphisme $\Phi : \left\{ \begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & \langle a, x\rangle a + \langle b, x\rangle b \end{array} \right.$

II.10 Eléments propres d'un endomorphisme (2) ★★★

[Corrigé]
Soit E l'espace des fonctions continues de $[0, 1]$ dans $\mathbb{R}$.

A toute application $f \in E$ on associe l'application

$$\Phi(f) : \left\{ \begin{array}{ccc} [0,1] & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \displaystyle\int_0^1 \min(x,t) f(t)\ dt \end{array} \right.$$

1. Montrer que Φ est un endomorphisme de E
2. Déterminer les éléments propres de Φ

II.11 Eléments propres d'un endomorphisme (3) ★★★

[Corrigé]
Soit $\mathcal{B}$ le sous-espace de $\mathbb{C}^{\mathbb{Z}}$ formé des suites bornées. On considère :

$$T : \left\{ \begin{array}{ccc} \mathcal{B} & \longrightarrow & \mathcal{B} \\ (u_n)_{n\in\mathbb{Z}} & \longmapsto & \left(\dfrac{u_{n-1}+u_{n+1}}{2}\right)_{n\in\mathbb{Z}} \end{array} \right.$$

1. Montrer que $T \in \mathcal{L}(\mathcal{B})$.
2. Déterminer les éléments propres de T

II.12 Eléments propres d'un endomorphisme (4) ★★★

[Corrigé]
Soit $E = \mathcal{C}(\mathbb{R}^+, \mathbb{R})$.
Pour $f \in E$ on définit l'application $T(f) : x \in \mathbb{R}_+^* \longmapsto \dfrac{1}{x}\displaystyle\int_0^x f(t)\ dt$

1. Soit $f \in E$. Montrer que $T(f)$ est prolongeable par continuité en 0 (on notera encore $T(f)$ le prolongement).
2. Déterminer les éléments propres de T.

II.13 Loi de Hooke ★★

[Corrigé]
Soit $\varphi : \left\{ \begin{array}{ccc} \mathcal{M}_n(\mathbb{R}) & \longrightarrow & \mathcal{M}_n(\mathbb{R}) \\ M & \longmapsto & M + \mathrm{Tr}(M) I_n \end{array} \right.$. Déterminer les éléments propres de φ.

II.14 Existence d'une valeur propre double ★★★

[Corrigé]
Soit $(A, B, C) \in \mathcal{M}_2(\mathbb{K})^3$.
Montrer qu'il existe $(\alpha, \beta, \gamma) \in (\mathbb{K}^*)^3$ tel que $\alpha A + \beta B + \gamma C$ admette une valeur propre double.

II.15 Détermination de spectre ★★★

[Corrigé]
On définit une suite de matrice par $A_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ et $A_{n+1} = \left(\begin{array}{c|c} A_n & A_n \\ \hline A_n & -A_n \end{array}\right)$.
Déterminer $\mathrm{Sp}(A_n)$.

II.16 Sommes et produits de valeurs propres

[Corrigé]
Soient $A, B \in \mathcal{M}_n(\mathbb{C})$.

1. Déterminer le spectre des applications linéaires suivantes :
$$\Phi : \left\{ \begin{array}{ccc} \mathcal{M}_n(\mathbb{C}) & \longrightarrow & \mathcal{M}_n(\mathbb{C}) \\ M & \longmapsto & AM + MB \end{array} \right. \qquad \Psi : \left\{ \begin{array}{ccc} \mathcal{M}_n(\mathbb{C}) & \longrightarrow & \mathcal{M}_n(\mathbb{C}) \\ M & \longmapsto & AMB \end{array} \right.$$
2. En déduire que l'ensemble des entiers algébriques (racines dans $\mathbb{C}$ d'un polynôme unitaire à coefficients entiers) est un sous-anneau de $\mathbb{C}$.

II.17 Matrice compagnon (1) ★★

[Corrigé]
Soit $P = X^n + \sum_{k=0}^{n-1} a_k X^k \in \mathbb{K}[X]$. On pose $C_P = \begin{pmatrix} 0 & \dots & \dots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \dots & 0 & 1 & -a_{n-1} \end{pmatrix}$.
Déterminer le polynôme caractéristique de C_P.

II.18 Réduction de la transposée d'une matrice ★

[Corrigé]
Soit $A \in \mathcal{M}_n(\mathbb{K})$.

1. Montrer que $\chi_A = \chi_{A^\top}$.
2. Montrer que $\forall \lambda \in \mathrm{Sp}(A),\ \dim E_\lambda(A) = \dim E_\lambda(A^\top)$.
3. En déduire que $A^\top$ est diagonalisable si et seulement A l'est.

II.19 Algorithme de Faddeev ★★★

[Corrigé]

Soit $A \in \mathcal{M}_n(\mathbb{K})$. Pour $\lambda \in \mathbb{K}$ on pose $B(\lambda) = \mathrm{Com}(\lambda I_n - A)^\top$.

1. Montrer qu'il existe des matrices $B_0, \dots, B_{n-1}$ de $\mathcal{M}_n(\mathbb{K})$ telles que :
$$B(\lambda) = \sum_{k=0}^{n-1} \lambda^{n-1-k} B_k$$
2. Montrer que $\chi_A'(\lambda) = \mathrm{Tr}(B(\lambda))$ Pour tout $\lambda \in \mathbb{K}$.
3. On pose $\chi_A = X^n - \sum_{k=1}^{n} p_k X^{n-k}$ et $B_n = 0$. Montrer que $\forall k \in [\![1; n-1]\!]$,
$$\begin{cases} p_k = \dfrac{1}{k}\mathrm{Tr}(AB_{k-1}) \\ B_k = AB_{k-1} - p_k I_n \end{cases}$$
et préciser B_0.
4. Montrer que si A est inversible alors $A^{-1} = \dfrac{1}{p_n} B_{n-1}$.
5. Ecrire un programme Python calculant le polynôme caractéristique d'une matrice A et un autre calculant son inverse à l'aide des questions précédentes.

II.20 Endomorphisme de transposition ★★

[Corrigé]

On pose $\Phi : \left\{ \begin{array}{ccc} \mathcal{M}_n(\mathbb{R}) & \longrightarrow & \mathcal{M}_n(\mathbb{R}) \\ M & \longmapsto & M^\top \end{array} \right.$.

Calculer $\det(\Phi)$ et $\mathrm{Tr}(\Phi)$.

II.21 Exemple de matrice non diagonalisable ★

[Corrigé]

1. Donner un exemple de matrice non diagonalisable sur $\mathbb{C}$.
2. Donner un exemple de matrice diagonalisable sur $\mathbb{C}$ mais pas sur $\mathbb{R}$.
3. La somme de deux matrices diagonalisables est-il diagonalisable ?
4. Le produit de deux matrices diagonalisables est-il diagonalisable ?

II.22 Diagonalisabilité d'une matrice (1) ★★★

[Corrigé]
Soit $(a_1, \dots, a_n) \in \mathbb{K}^n$.

A quelle condition la matrice $A = \begin{pmatrix} 0 & 0 & \dots & 0 & a_1 \\ 0 & \ddots & & 0 & a_2 \\ \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & a_{n-1} \\ a_1 & a_2 & \dots & a_{n-1} & a_n \end{pmatrix}$ est-elle diagonalisable ?

II.23 Diagonalisabilité d'une matrice (2) ★★★

[Corrigé]
La matrice $A = (i/j)_{1 \leq i,j \leq n}$ est-elle diagonalisable ?

II.24 Diagonalisabilité d'une matrice (3) ★★★

[Corrigé]
Soient $U \in \mathcal{M}_n(\mathbb{C})$ et $V = \left(\begin{array}{c|c} 0 & I_n \\ \hline U & 0 \end{array}\right)$.
Déterminer une condition nécessaire et suffisante sur U pour que V soit diagonalisable.

II.25 Cotrigonalisation (1) ★★★

[Corrigé]
Soit E un $\mathbb{K}$-espace vectoriel de dimension n finie.

1. Soient $u, v \in \mathcal{L}(E)$ trigonalisables et commutant.
   Montrer que u et v admettent une base de trigonalisation commune.
2. Soient $u_1, \dots, u_p \in \mathcal{L}(E)$ trigonalisables et commutant deux à deux.
   Montrer que $u_1, \dots, u_n$ admettent une base de trigonalisation commune.
3. Soit $\mathcal{A}$ une sous-algèbre commutative de $\mathcal{L}(E)$ formée d'endomorphismes trigonalisables.
   Montrer qu'il existe une base de trigonalisation commune à tous les éléments de $\mathcal{A}$.

II.26 Cotrigonalisation (2) ★★★

[Corrigé]
Soit E un $\mathbb{C}$-espace vectoriel de dimension n finie. On note E^* l'espace dual de E.

Pour $u \in \mathcal{L}(E)$ on pose $T_u : \left\{ \begin{array}{ccc} E^* & \longrightarrow & E^* \\ \Phi & \longmapsto & \Phi \circ u \end{array} \right.$.

On fixe $(u, v) \in \mathcal{L}(E)^2$.

1. Montrer que $T_u \in \mathcal{L}(E^*)$.
2. Donner une condition suffisante pour que T_u et T_v commutent.
3. On suppose que u et v commutent. Montrer que u et v sont trigonalisables dans une même base.

II.27 Cotrigonalisation (3) ★★★★

[Corrigé]

Soient A, B, C trois matrices de $\mathcal{M}_n(\mathbb{C})$ telles que

$$AB - BA = C, \ AC = CA, \ BC = CB$$

1. Montrer que A, B et C ont un vecteur propre commun.
2. Montrer que A, B, C sont cotrigonalisables.

II.28 Cotrigonalisation (4) ★★★★

[Corrigé]

Soient $A, B \in \mathcal{M}_n(\mathbb{C})$.

1. On suppose qu'il existe $\lambda \in \mathbb{C}^*$ tel que $AB - BA = \lambda A$.
   Montrer que A est nilpotente. En déduire que A et B ont un vecteur propre commun.
2. On suppose qu'il existe $\lambda, \mu \in \mathbb{C}$ tels que $AB - BA = \lambda A + \mu B$.
   Montrer que A et B possèdent un vecteur propre commun. En déduire que A et B sont cotrigonalisables.

II.29 Cotrigonalisation (5) ★★★

[Corrigé]

Soit $(A, B) \in \mathcal{M}_n(\mathbb{C})^2$ tel que $AB = 0$. Montrer que A et B sont cotrigonalisables.

II.30 Caractérisation des matrices nilpotente par la trace ★★★

[Corrigé]

Soit $A \in \mathcal{M}_n(\mathbb{K})$ Montrer que A est nilpotente si et seulement si $\forall k \in \mathbb{N}^*, \ \mathrm{Tr}\,(A^k) = 0$.

II.31 Facteur commun dans le polynôme caractéristique ★★★

[Corrigé]
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Soit $(f,g) \in \mathcal{L}(E)^2$.
On suppose qu'il existe $h \in \mathcal{L}(E)$ de rang $r \geq 1$ tel que $f \circ h = h \circ g$.
Montrer que χ_f et χ_g ont un facteur commun de degré r.
La réciproque est-elle vraie ?

II.32 $\chi_{AB} = \chi_{BA}$ ★★★

[Corrigé]
Soient $\lambda \in \mathbb{K}$, $A \in \mathcal{M}_{n,p}(\mathbb{K})$ et $B \in \mathcal{M}_{p,n}(\mathbb{K})$. On pose

$$M = \left(\begin{array}{c|c} \lambda I_n & -A \\ \hline -B & I_p \end{array}\right)$$

1. Etablir que $\lambda^p \chi_{AB}(\lambda) = \lambda^n \chi_{BA}(\lambda)$.

2. En déduire que $\chi_{AB} = \chi_{BA}$ si $n = p$.

II.33 Polynôme caractéristique de l'inverse ★★

[Corrigé]
Soit $A \in \mathrm{GL}_n(\mathbb{K})$. Exprimer $\chi_{A^{-1}}$ en fonction de χ_A.

II.34 Commutativité et stabilité ★★

[Corrigé]
Soient u et v deux endomorphismes d'un $\mathbb{K}$-espace vectoriel de dimension finie E. On suppose u diagonalisable.
Montrer que u et v commutent si et seulement si tout sous-espace propre de u est stable par v.

II.35 Dimension du commutant d'une matrice diagonalisable ★★★

[Corrigé]
Soit $A \in \mathcal{M}_n(\mathbb{K})$ diagonalisable.
On note $\mathrm{Sp}(A) = \{\lambda_1, \dots, \lambda_r\}$ ainsi que $n_1 \dots, n_r$ leur multiplicité respective.
On note également $\mathcal{C}(A) = \{M \in \mathcal{M}_n(\mathbb{K}),\ AM = MA\}$ le commutant de A.

1. Montrer que $\dim \mathcal{C}(A) = \sum_{\lambda \in \mathrm{Sp}(A)} \dim E_\lambda(A)^2$
2. En déduire que $\dim \mathcal{C}(A) = n \iff \dim \mathbb{K}[A] = n \iff r = n \iff \mathcal{C}(A) = \mathbb{K}[A]$.

II.36 Sous-espaces stables d'un endomorphisme diagonalisabl ★★★

[Corrigé]
Soit u un endomorphisme diagonalisable d'un $\mathbb{K}$-espace vectoriel E de dimension finie.

1. Soit F un sous-espace vectoriel de E. On pose $G = \bigoplus_{\lambda \in \mathrm{Sp}(u)} F \cap E_\lambda(u)$.
   Montrer que G est stable par u.
2. Soit F un sous-espace vectoriel de E stable par u. Montrer que $F = \bigoplus_{\lambda \in \mathrm{Sp}(u)} F \cap E_\lambda(u)$
3. Montrer que les sous-espaces vectoriels de E stables par u sont exactement ceux de la forme $\bigoplus_{\lambda \in \mathrm{Sp}(u)} F_\lambda$ où pour tout $\lambda \in \mathrm{Sp}(u)$, F_λ est un sous-espace vectoriel de $E_\lambda(u)$.

II.37 Hyperplans stables ★★★

[Corrigé]
Soient E un $\mathbb{R}$-espace vectoriel de dimension n et $f \in \mathcal{L}(E)$.
Montrer que f est diagonalisable si et seulement s'il existe des hyperplans $H_1, \dots, H_n$ de E stables par f tels que $\bigcap_{i=1}^{n} H_i = \{0_E\}$.

II.38 Endomorphisme qui stabilise un nombre fini de sous-espaces ★★★

[Corrigé]
Soit u un endomorphisme à spectre simple d'un $\mathbb{K}$-espace vectoriel E de dimension n finie. (c'est à dire que u a exactement n valeurs propres distinctes)
Montrer qu'il existe un nombre fini de sous-espaces de E stables par u et les dénombrer.

II.39 Sous-espaces stables d'un endomorphisme nilpotent maximal ★★★

[Corrigé]
Soit E un $\mathbb{K}$-espace vectoriel de dimension n finie.
On considère $u \in \mathcal{L}(E)$ nilpotent d'indice n.
Montrer que u stabilise exactement $n+1$ sous-espaces vectoriels de E.

II.40 Sous-espaces stables par les endomorphismes de permutation ★★★★

[Corrigé]
Soit $\sigma \in \mathcal{S}_n$. On définit l'endomorphisme $u_\sigma : (x_1, \dots, x_n) \in \mathbb{C}^n \mapsto (x_{\sigma(1)}, \dots, x_{\sigma(n)})$.

1. Déterminer le spectre de u_σ.
2. Déterminer les sous-espaces vectoriels de $\mathbb{C}^n$ stables par tous les $u_\sigma,\ \sigma \in \mathcal{S}_n$.

II.41 Semi-simplicité ★★★

[Corrigé]
Soit u un endomorphisme d'un $\mathbb{C}$-espace vectoriel E de dimension finie.
Montrer que u est diagonalisable si et seulement si tout sous-espace vectoriel de E admet un supplémentaire dans E stable par u. Le résultat persiste t-il pour des $\mathbb{R}$-espaces vectoriels ?

II.42 Endomorphismes diagonalisables d'un $\mathbb{R}$-espace vectoriel ★★★

[Corrigé]
Soient f, g deux endomorphismes diagonalisables d'un $\mathbb{R}$-espace vectoriel E de dimension n finie. Soit également k un entier naturel impair.

1. Montrer que tout vecteur propre de f^k est vecteur propre de f.
2. Montrer que $f^k = g^k \implies f = g$.

II.43 Matrices à spectres disjoints ★★★

[Corrigé]

Soient $A, B \in \mathcal{M}_n(\mathbb{K})$.

Montrer l'équivalence des propositions suivantes :

(i) A et B n'ont pas valeurs propres communes ;

(ii) $\chi_A(B)$ est inversible ;

(iii) $\forall X \in \mathcal{M}_n(\mathbb{K}),\ AX = XB \implies X = 0$;

(iv) $\forall M \in \mathcal{M}_n(\mathbb{K}), \exists X \in \mathcal{M}_n(\mathbb{K}),\ AX - XB = M$.

III Réduction algébrique

Dans toute cette section n désigne un entier supérieur ou égal à 1.

III.1 Equation matricielle polynomiale (1) ★★

[Corrigé]
Déterminer les matrices $M \in \mathcal{M}_n(\mathbb{C})$ vérifiant $M^5 = M^2$ et $\mathrm{Tr}(M) = n$.

III.2 Equation matricielle polynomiale (2) ★★

[Corrigé]
Soit $A \in \mathcal{M}_n(\mathbb{R})$ telle que $A^3 + A^2 + A = 0$. Montrer que $\mathrm{rg}(A)$ est pair.

III.3 Equation matricielle avec la comatrice ★★★★

[Corrigé]

1. Montrer que $\forall A, B \in \mathcal{M}_n(\mathbb{C}),\ \mathrm{Com}(AB) = \mathrm{Com}(A)\,\mathrm{Com}(B)$.

On cherche les matrices $A \in \mathcal{M}_n(\mathbb{C})$ telles que $A + \mathrm{Com}(A)^\top$ soit une matrice scalaire. Pour $\lambda \in \mathbb{C}$ on note $E_\lambda = \{A \in \mathcal{M}_n(\mathbb{C}),\ A + \mathrm{Com}(A)^\top = \lambda I_n\}$.

2. Montrer que si $A \in E_\lambda$ alors toute la classe de conjugaison de A est dans E_λ.
3. Discuter du rang de $\mathrm{Com}(A)$ en fonction du rang de A.
4. En déduire l'ensemble des matrices recherchées.

III.4 Rang et spectre de la comatrice ★★★

[Corrigé]
Soit $A \in \mathcal{M}_n(\mathbb{C})$. Déterminer le rang et le spectre de $\tilde{A} = \mathrm{Com}(A)^\top$.

III.5 Racine p-ième d'une matrice ★★★

[Corrigé]
Soient $A \in \mathrm{GL}_n(\mathbb{C})$ diagonalisable, $B \in \mathcal{M}_n(\mathbb{C})$ et $p \in \mathbb{N}^*$ tels que $B^p = A$.
Montrer que B est diagonalisable. Le résultat persiste-il avec A non inversible ?

III.6 Diagonalisibilité de f dans le cas f^2 diagonalisable ★★★

[Corrigé]

1. Soit $f \in \mathcal{L}(\mathbb{C}^n)$. Montrer que f est diagonalisable si et seulement si f^2 est diagonalisable et $\ker f = \ker f^2$.
2. Soit $f \in \mathcal{L}(\mathbb{R}^n)$ tel que f^2 est diagonalisable. A quelle condition nécessaire et suffisante f est-il diagonalisable ?
3. Soit $(a_1, \dots, a_n) \in \mathbb{C}^n$.

   A quelle condition nécessaire et suffisante la matrice $A = \begin{pmatrix} 0 & \dots & 0 & a_n \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ddots & \ddots & \vdots \\ a_1 & 0 & \dots & 0 \end{pmatrix}$ est-elle diagonalisable dans $\mathcal{M}_n(\mathbb{C})$? Dans $\mathcal{M}_n(\mathbb{R})$?

III.7 Endomorphismes diagonalisables non bijectifs ★★

[Corrigé]
Soient E un $\mathbb{K}$-espace vectoriel et $f \in \mathcal{L}(E)$.

1. On suppose qu'il existe $P \in \mathbb{K}[X]$ un polynôme annulateur de f tel que $P(0) = 0$ et $P'(0) \neq 0$. Montrer que $E = \mathrm{Ker} f \bigoplus \mathrm{Im} f$.
2. On suppose f diagonalisable et non bijectif. Montrer que $E = \mathrm{Ker} f \bigoplus \mathrm{Im} f$.

III.8 Valuation du polynôme minimal ★★★

[Corrigé]
Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et $f \in \mathcal{L}(E)$. On note p la valuation de π_f (i.e le plus petit degré des monômes non nuls de π_f).

1. On suppose que $p = 0$. Que peut-on dire de f ?
2. Montrer que $E = \mathrm{Ker}(f^p) \bigoplus \mathrm{Im}(f^p)$.
3. On suppose $p \neq 0$. Montrer que p est le plus petit entier naturel non nul vérifiant l'égalité précédente.

III.9 Sous-espaces stables ★★★

[Corrigé]
Soient u un endomorphisme d'un $\mathbb{K}$-espace vectoriel de dimension finie et $P \in \mathbb{K}[X]$ un polynôme unitaire annulateur de u. La décomposition de P en facteurs irréductibles unitaires s'écrit $P = \prod_{i=1}^{r} P_i$. Pour $i \in [\![1; r]\!]$, on pose $N_i = \ker P_i(u)$.

Soit F un sous-espace vectoriel de E stable par u. Montrer que $F = \bigoplus_{i=1}^{r} F \cap N_i$.

III.10 Une formule sur les polynômes ★★★

[Corrigé]
Montrer que $\forall P \in \mathbb{C}_{n-1}[X]$, $\sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} P(X+k) = 0$.

III.11 Ordre de matrice ★★★★

[Corrigé]
Soit $M \in \mathrm{GL}_2(\mathbb{Z})$. On note $\chi_M = X^2 - tX + d$ le polynôme caractéristique de M.
En discutant les valeurs possibles de t et d, déterminer tous les ordres possibles pour M, puis trouver un exemple pour chaque ordre.

III.12 Sous-groupes finis de $\mathrm{GL}_2(\mathbb{Z})$ ★★★★

[Corrigé]
On note $\mathrm{GL}_2(\mathbb{Z})$ l'ensemble des matrices inversibles de $\mathcal{M}_2(\mathbb{Z})$ dont l'inverse est aussi dans $\mathcal{M}_2(\mathbb{Z})$.

1. Montrer que $(\mathrm{GL}_2(\mathbb{Z}), \times)$ est un groupe.
2. Soit G un sous-groupe fini de $\mathrm{GL}_2(\mathbb{Z})$.
   Montrer que $\forall M \in G,\ M^{12} = I_2$.

III.13 Sous-groupes finis de $\mathrm{GL}_n(\mathbb{Z})$ ★★★★

[Corrigé]
On note $\mathrm{GL}_n(\mathbb{Z}) = \{M \in \mathcal{M}_n(\mathbb{Z}),\ (M, M^{-1}) \in \mathcal{M}_n(\mathbb{Z})^2\}$.

1. Soit $M \in \mathcal{M}_n(\mathbb{Z})$. Montrer que $M \in \mathrm{GL}_n(\mathbb{Z})$ si et seulement si $|\det M| = 1$.
   Montrer que $\mathrm{GL}_n(\mathbb{Z})$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.
2. Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$.
   a. On fixe $M \in G$ et on pose $N = \frac{1}{3}(M - I_n)$. Etudier la convergence de la suite $(N^k)_{k\in\mathbb{N}}$.
   b. On utilisant l'application $\pi : \left\{ \begin{array}{ccc} \mathcal{M}_n(\mathbb{Z}) & \longrightarrow & \mathcal{M}_n(\mathbb{Z}/3\mathbb{Z}) \\ A & \longmapsto & \overline{A} \end{array} \right.$, Montrer qu'il existe un entier K_n tel que $|G| \leq K_n$.

III.14 Isomorphisme entre $\mathrm{GL}_n(\mathbb{C})$ et $\mathrm{GL}_m(\mathbb{C})$ ★★★★

[Corrigé]

1. On se donne p matrices $A_1, \dots, A_p \in \mathcal{M}_n(\mathbb{C})$ diagonalisables et commutant entre elles.
   a. Montrer que A_1 et A_2 sont codiagonalisables.
   b. Montrer que $A_1, \dots, A_p$ sont codiagonalisables.
2. Soit G un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$ tel que $\forall A \in G,\ A^2 = I_n$. Montrer que G est fini. Que dire de son cardinal ?
3. Soient $m, n \in \mathbb{N}^*$ distincts. Existe-il un isomorphisme de $\mathrm{GL}_n(\mathbb{C})$ sur $\mathrm{GL}_m(\mathbb{C})$?

III.15 Inverse et conjugaison ★★★★★

[Corrigé]
Soit $A \in \mathcal{M}_n(\mathbb{C})$. Montrer que $A\overline{A} = I_n \iff \exists S \in \mathrm{GL}_n(\mathbb{C}),\ A = S\overline{S}^{-1}$.

III.16 Matrice compagnon (2) ★★

[Corrigé]

Soit $(a_0, \dots, a_n) \in \mathbb{K}^n$. On pose $A = \begin{pmatrix} 0 & \dots & \dots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \dots & 0 & 1 & -a_{n-1} \end{pmatrix}$.

1. Montrer que $\chi_A = X^n + \sum_{k=0}^{n-1} a_k X^k$
2. Montrer que $\pi_A = \chi_A$
3. Déterminer les sous-espaces propres de $A^\top$.

III.17 Polynôme minimal ponctuel ★★★

[Corrigé]

Soit u un endomorphisme d'un $\mathbb{K}$-espace vectoriel E de dimension n.

1. Pour $x \in E$ on note $I_{u,x} = \{P \in \mathbb{K}[X],\ P(u)(x) = 0_E\}$ et $E_{u,x} = \{P(u)(x),\ P \in \mathbb{K}[X]\}$. On fixe $x \in E$.
   a. Montrer que $I_{u,x}$ est un idéal de $\mathbb{K}[X]$. On note $\pi_{u,x}$ son unique générateur unitaire (appelé polynôme minimal ponctuel de u en x).
   b. Montrer que $E_{u,x}$ est un sous-espace vectoriel de E et que $(u^k(x))_{0 \leq k \leq \deg(\pi_{u,x})-1}$ en est une base.
2. Soient $x_1, \dots, x_p \in E$ tels que leur polynômes minimaux ponctuels associés soient premiers entre eux. On pose $x = \sum_{i=1}^{p} x_i$ et $P = \prod_{i=1}^{p} \pi_{u,x_i}$.
   a. Montrer que $\pi_{u,x}$ divise P.
   b. Montrer que les sous-espaces vectoriels $E_{u,x_1}, \dots, E_{u,x_p}$ sont en somme directe.
   c. En déduire que $\pi_{u,x} = P$ et $E_{u,x} = \bigoplus_{i=1}^{p} E_{u,x_i}$.
3. En considérant la décomposition en facteurs irréductibles de $\pi_{u,x}$, montrer à l'aide de la question précédente qu'il existe $x \in E$ tel que $\pi_{u,x} = \pi_u$.
4. Montrer que les conditions suivantes sont équivalentes.
   (i) $\pi_u = \chi_u$;
   (ii) Il existe $x \in E$ tel que $E_{u,x} = E$;

(iii) Il existe une base de E dans laquelle la matrice de u est de la forme

$$\begin{pmatrix} 0 & \dots & \dots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \dots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

On dit dans ce cas que u est un endomorphisme cyclique.

III.18 Endomorphismes cycliques ★★★

[Corrigé]

Soit E un $\mathbb{K}$-espace vectoriel de dimension n. On dit d'un endomorphisme f de E qu'il est cyclique lorsqu'il existe un vecteur $x_0 \in E$ tel que la famille $(x_0, f(x_0), \dots, f^{n-1}(x_0))$ soit une base de E.

Pour $Q = X^n + \sum_{k=0}^{n-1} a_k X^k$ on pose

$$C_Q = \begin{pmatrix} 0 & \dots & \dots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \dots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

sa matrice compagnon.

1. Montrer que $f \in \mathcal{L}(E)$ est cyclique si et seulement s'il existe un polynôme Q unitaire de degré n et une base de E dans laquelle la matrice de f est C_Q.
2. a. Soit $M \in \mathcal{M}_n(\mathbb{K})$. Montrer que M est diagonalisable si et seulement si $M^\top$ l'est.
   b. Soit $Q \in \mathbb{K}[X]$ unitaire de degré n. Déterminer la dimension des sous-espaces propres de $C_Q^\top$ et en déduire une condition nécessaire et suffisante pour qu'un endomorphisme cyclique soit diagonalisable.

III.19 Commutant d'un endomorphisme cyclique ★★★

[Corrigé]

Soit E un $\mathbb{K}$-espace vectoriel de dimension n. On se donne $f \in \mathcal{L}(E)$ et $x_0 \in E$ tel que

$\mathcal{B} = (x_0, f(x_0), \dots, f^{n-1}(x_0))$ soit une base de E. On note $\mathcal{C}(f) = \{g \in \mathcal{L}(E),\ f \circ g = g \circ f\}$ le commutant de f.

Soit $g \in \mathcal{C}(f)$. On note $g(x_0) = \sum_{k=0}^{n-1} \lambda_k f^k(x_0)$ la décomposition de $g(x_0)$ dans la base $\mathcal{B}$.

1. Montrer que $g \in \mathbb{K}[f]$.
2. Montrer que $\mathcal{C}(f) = \mathbb{K}_{n-1}[f]$.

III.20 Une démonstration de Cayley-Hamilton ★★★

[Corrigé]

Soient x un vecteur non nul d'un $\mathbb{K}$-espace vectoriel E de dimension n et $f \in \mathcal{L}(E)$.

1. Montrer qu'il existe un entier $p \in \mathbb{N}^*$ pour lequel $(x, f(x), \dots, f^{p-1}(x))$ est libre et il existe $(\alpha_0 \dots, \alpha_{p-1}) \in \mathbb{K}^p$ tel que :
$$\alpha_0 x + \alpha_1 f(x) + \cdots + \alpha_{p-1} f^{p-1}(x) + f^p(x) = 0$$
2. Justifier que $\mathrm{Vect}(x, f(x) \dots, f^{p-1}(x))$ est stable par f.
3. Montrer que $P = X^p + \sum_{k=0}^{p-1} \alpha_k X^k$ divise χ_f. (On pourra déterminer le polynôme caractéristique de la matrice compagnon de P cf. II.17)
4. En déduire le théorème de Cayley-Hamilton.

III.21 Indépendance de corps du polynôme minimal ★★★

[Corrigé]

Soit $M \in \mathcal{M}_n(\mathbb{R})$. Montrer que le polynôme minimal de M, vu comme une matrice à coefficients réels, est le même que celui de M, vu comme une matrice à coefficients complexes.

III.22 Polynôme minimal de l'inverse ★★★

[Corrigé]

1. Soit $A \in \mathrm{GL}_n(\mathbb{R})$. Exprimer le polynôme minimal de A^{-1} en fonction de celui de A.
2. Soit $A \in \mathcal{O}_n(\mathbb{R})$ telle que 1 et -1 ne soient pas valeurs propres de A. Montrer que le polynôme minimal de A est de degré pair.

III.23 Polynôme minimal de la transposée ★

[Corrigé]
Montrer qu'une matrice et sa transposée ont même polynôme minimal.

III.24 Polynôme minimal imposé ★★★

[Corrigé]
Le polynôme $X^4 + X^3 + 2X^2 + X + 1$ peut-il être le polynôme minimal d'une matrice de $\mathcal{M}_5(\mathbb{R})$?

III.25 Matrice de Gram ★★★

[Corrigé]
Soit E un espace euclidien.
A toute famille $(x_1, \dots, x_p)$ de p vecteurs de E on associe la matrice $G(x_1, \dots, x_p) = (\langle x_i, x_j \rangle)_{1 \leq i,j \leq p}$.

1. Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base orthonormée de $\mathcal{F} = \text{Vect}(x_1, \dots, x_p)$. On note $A = \text{mat}_{\mathcal{B}}(x_1, \dots, x_p)$.
   Montrer que $G(x_1, \dots, x_p) = A^\top A$.
2. En déduire que les valeurs propres de G sont positives ou nulles.
3. Montrer que chaque valeur propre de G est majorée par $\sum_{i=1}^{p} \|x_i\|^2$.

III.26 Matrice circulante ★★★

[Corrigé]
Soit $(a_0, \dots, a_{n-1}) \in \mathbb{C}^n$.

On note $A = \begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & a_2 \\ a_2 & & \ddots & \ddots & a_1 \\ a_1 & a_2 & \dots & a_{n-1} & a_0 \end{pmatrix} \in \mathcal{M}_n(\mathbb{C})$

et $J = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 0 \\ 0 & \dots & \dots & 0 & 1 \\ 1 & 0 & \dots & \dots & 0 \end{pmatrix} \in \mathcal{M}_n(\mathbb{C})$

1. Calculer J^k pour $k \in \mathbb{N}$.
2. Diagonaliser A.

III.27 Diagonalisabilité du produit de deux matrices ★★★

[Corrigé]
Soit $(A, B) \in \mathcal{M}_{n,p}(\mathbb{K}) \times \mathcal{M}p, n\mathbb{K}$. On suppose que AB est diagonalisable et inversible. Montrer que BA est diagonalisable

— avec des arguments de réduction algébrique

— avec des arguments de réduction géométrique

III.28 Diagonalisation d'une matrice par bloc ★★★

[Corrigé]
Soient $A \in \mathcal{M}_n(\mathbb{K})$ et $M = \left(\begin{array}{c|c} A & 0 \\ \hline A & A \end{array}\right)$.

1. Comparer le spectre de M à celui de A.
2. Soit $P \in \mathbb{K}[X]$. Exprimer $P(M)$ en fonction de $P(A)$ et de $P'(A)$.
3. Donner une condition portant sur A nécessaire et suffisante à ce que M soit diagonalisable.

III.29 Exponentielle matricielle ★★★

[Corrigé]

1. Montrer que $A \in S_n(\mathbb{R}) \implies \exp(A) \in S_n(\mathbb{R})$.
2. Montrer que $A \in A_n(\mathbb{R}) \implies \exp(A) \in \mathrm{SO}_n(\mathbb{R})$.

III.30 Exponentiel d'un endomorphisme nilpotent ★★★

[Corrigé]
Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in \mathcal{L}(E)$ nilpotent. Montrer que $\mathrm{Ker}(\exp(u) - \mathrm{Id}_E) = \mathrm{Ker}(u)$ et $\mathrm{Im}(\exp(u) - \mathrm{Id}_E) = \mathrm{Im}(u)$.

III.31 Endomorphismes anticommutants ★★★★

[Corrigé]
Soient p un entier supérieur ou égal à 2, E un $\mathbb{C}$-espace vectoriel de dimension n et $u_1, \dots, u_p \in \mathcal{L}(E)$ vérifiant :

$$\forall k \in [\![1;p]\!],\ u_k^2 = -\operatorname{Id}_E \text{ et } \forall (i,j) \in [\![1;p]\!]^2, (i \neq j \implies u_i \circ u_j = -u_j \circ u_i)$$

Calculer le déterminant de chacun des u_k.

III.32 Trace entière ★★★★

[Corrigé]
Caractériser les polynômes $P \in \mathbb{C}[X]$ tels que : $\forall A \in \mathcal{M}_n(\mathbb{C}),\ P(A) = 0 \implies \operatorname{Tr}(A) \in \mathbb{Z}$.

III.33 $P(A)$ nilpotente ★★★

[Corrigé]
Soit $A \in \mathcal{M}_n(\mathbb{C})$. Déterminer les polynômes $P \in \mathbb{C}[X]$ tels que $P(A)$ soit nilpotente.

IV Déterminant

Dans toute cette section n désigne un entier supérieur ou égal à 1.

IV.1 Dimension de l'espace des formes multilinéaires alternées ★★★★

[Corrigé]
Soit E un $\mathbb{K}$-espace vectoriel de dimension d. Soit $n \in \mathbb{N}^*$.
On appelle forme n-linéaire alternée sur E toute application $f : E^n \to \mathbb{K}$ telle que :

— f est linéaire par rapport à chacune de ses variables ;

— $\forall \sigma \in \mathcal{S}_n,\ \forall (x_1, \dots, x_n) \in E^n,\ f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \varepsilon(\sigma) f(x_1, \dots, x_n)$.

On note $\mathcal{A}_n(E)$ l'ensemble des formes n-linéaires alternées sur E.

1. Donner un élément de $\mathcal{A}_d(E)$.
2. Montrer que $\mathcal{A}_n(E)$ est un $\mathbb{K}$-espace vectoriel et en déterminer la dimension.

IV.2 Théorème de Bézout matriciel ★★

[Corrigé]
Soient $A, B \in \mathcal{M}_n(\mathbb{Z})$.

1. Montrer que $\det(A), \det(B) \in \mathbb{Z}$.
2. On suppose que $\det(A)$ et $\det(B)$ sont premiers entre eux.
   Montrer qu'il existe deux matrices $U, V \in \mathcal{M}_n(\mathbb{Z})$ telles que $AU + BV = I_n$.

IV.3 Déterminant tridiagonal ★★★

[Corrigé]
Soit $(a,b,c) \in \mathbb{C}^3$.

Calculer $\Delta_n = \begin{vmatrix} a & c & 0 & \dots & 0 \\ b & a & c & \ddots & \vdots \\ 0 & b & a & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & c \\ 0 & \dots & 0 & b & a \end{vmatrix}_n$

IV.4 Déterminant bitriangulaire ★★★

[Corrigé]
Soit $(a,b) \in \mathbb{C}^2$ avec $a \neq b$.

Calculer le déterminant de $M = \begin{pmatrix} 0 & & (a) \\ & \ddots & \\ (b) & & 0 \end{pmatrix} \in \mathcal{M}_n(\mathbb{C})$.

IV.5 Déterminant de Vandermonde ★

[Corrigé]

Pour $(x_1,\dots,x_n) \in \mathbb{K}^n$ on définit $V(x_1,\dots,x_n) = \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix}$

Calculer $V(x_1,\dots,x_n)$.
On pourra étudier pour $(x_1,\dots,x_{n-1}) \in \mathbb{K}^{n-1}$ fixée $f : x \longmapsto V(x_1,\dots,x_{n-1},x)$

IV.5.1 Utilisation du déterminant de Vandermonde

Calculer le déterminant :

$$\begin{vmatrix} a_1+a_2 & a_2+a_3 & \dots & a_n+a_1 \\ a_1^2+a_2^2 & a_2^2+a_3^2 & \dots & a_n^2+a_1^2 \\ \vdots & \vdots & & \vdots \\ a_1^n+a_2^n & a_2^n+a_3^n & \dots & a_n^n+a_1^n \end{vmatrix}$$

IV.6 Déterminant de Hilbert ★★★

[Corrigé]

Notons $H_n = \left(\frac{1}{i+j+1}\right)_{0\leq i,j\leq n-1}$

1. On pose pour tout x réel, $\Delta_n(x) = \begin{vmatrix} 1 & \frac{1}{2} & \frac{1}{3} & \cdots & \frac{1}{n} \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \cdots & \frac{1}{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{1}{n-1} & \frac{1}{n} & \frac{1}{n+1} & \cdots & \frac{1}{2n-2} \\ \frac{1}{x} & \frac{1}{x+1} & \frac{1}{x+1} & \cdots & \frac{1}{x+n-1} \end{vmatrix}$

   a. Montrer qu'il existe $Q_n \in \mathbb{R}_{n-1}[X]$ tel que $\Delta_n(X) = \dfrac{Q_n(X)}{X(X+1)(X+2)\dots(X+n-1)}$

   b. Montrer qu'il existe $\lambda_n \in \mathbb{R}$ tel que $Q_n(X) = \lambda_n(X-1)(X-2)\dots(X-n+1)$

2. Vérifier que $\det H_n = \dfrac{2^n n!}{(2n)!}\displaystyle\prod_{k=1}^{n-1}\frac{(k!)^4}{((2k)!)^2}$

IV.7 Déterminant de Gram ★★★

[Corrigé]

Soit E un espace euclidien. A toute famille $(x_1,\dots,x_p)$ de p vecteurs de E on associe la matrice
$G(x_1,\dots,x_p) = (\langle x_i, x_j\rangle)_{1\leq i,j\leq p}$.

1. Soit $\mathcal{B} = (e_1,\dots,e_n)$ une base orthonormée de $\mathcal{F} = \text{Vect}(x_1,\dots,x_p)$. On note $A = \text{mat}_{\mathcal{B}}(x_1,\dots,x_p)$.
   Montrer que $G(x_1,\dots,x_p) = A^\top A$.

2. En déduire que $(x_1,\dots,x_p)$ est liée si et seulement si $\det G(x_1,\dots,x_p) = 0$ puis que :
   $\forall x \in E,\ \det G(x_1,\dots,x_p,x) = d(x,\mathcal{F})^2 \det G(x_1,\dots,x_p)$.

IV.8 Déterminant de Cauchy ★★★

[Corrigé]

Pour toutes familles $(a_k)_{1\leq k\leq n}$ et $(b_k)_{1\leq k\leq n}$ de complexes telles que $a_k + b_k \neq 0$ pour tout $k \in [\![1;n]\!]$, on définit $C_n = C(a_1,\dots,a_n,b_1,\dots,b_n) = \det\left(\dfrac{1}{a_i+b_j}\right)_{1\leq i,j\leq n}$.

1. On pose $F(X) = C(a_1, \dots, a_{n-1}, X, b_1, \dots, b_n)$.
   Montrer qu'il existe $P \in \mathbb{C}_{n-1}[X]$ tel que $F(X) = \dfrac{P(X)}{\prod_{i=1}^{n}(X + b_i)}$.

2. a. Déterminer les racines de P.
   b. Exprimer le coefficient dominant de P en fonction de C_{n-1}.
   (On pourra s'intéresser à $(X + b_n)F(X)$)

3. Calculer C_n.

IV.9 Déterminant de Smith ★★★

[Corrigé]

1. On pose $A = (a_{ij})_{1 \leq i,j \leq n}$ avec $a_{ij} = \begin{cases} 1 & \text{si } j|i \\ 0 & \text{sinon} \end{cases}$
   Calculer le déterminant de A.

2. On pose $D = (d_{ij})_{1 \leq i,j \leq n}$ avec d_{ij} le nombre de diviseurs communs à i et j.
   Calculer le déterminant de D.

3. On pose $S = (i \wedge j)_{1 \leq i,j \leq n}$
   Montrer que $\det S = \prod_{k=1}^{n} \varphi(k)$ où φ désigne l'indicatrice d'Euler.
   On pourra admettre la formule classique $n = \sum_{d|n} \varphi(d)$.

IV.10 Déterminant de Cayley-Menger ★★★★

[Corrigé]
Soient $x_0, \dots, x_n$ des points de $\mathbb{R}^n$ et $d_{i,j} = \|x_j - x_i\|$ les distances associées.

On pose $\Gamma(x_0, \dots, x_n) = \begin{vmatrix} 0 & 1 & \dots & 1 \\ 1 & \ddots & d_{i,j}^2 & \\ \vdots & d_{i,j}^2 & \ddots & \\ 1 & & & 0 \end{vmatrix}$ Démontrer que :

$$\det(x_1 - x_0, \dots, x_n - x_0)^2 = \frac{(-1)^{n+1}}{2^n} \Gamma(x_0, \dots, x_n)$$

Remarque : Ce résultat permet de calculer le volume du simplexe (généralisation du triangle à une dimension quelconque).

Cette formule se simplifie en dimension 2. On reconnaît la formule de Héron d'Alexandrie : la surface S d'un triangle de côté a, b, c vérifie la relation

$$S^2 = p(p-a)(p-b)(p-c)$$

où p est le demi périmètre.

V Groupes

V.1 Existence d'un idempotent ★★★

[Corrigé]
Soit $(E, \cdot)$ un semi-groupe (c'est à dire que la loi $\cdot$ est une loi de composition interne associative sur E) non vide et fini.
Montrer qu'il existe $s \in E$ tel que $s \cdot s = s$.

V.2 Sous-semi-groupes finis de $\mathcal{M}_n(\mathbb{K})$

[Corrigé]
Soit $(U, \cdot)$ un sous-semi-groupe de $\mathcal{M}_n(\mathbb{K})$ (i.e U est stable par produit) non vide et fini.
Montrer que $\exists A \in U,\ \mathrm{Tr}(A) \in [\![0; n]\!]$.

V.3 Groupe d'exposant inférieur à 2 ★

[Corrigé]
Soit G un groupe de neutre e pour lequel, $\forall x \in G,\ x^2 = e$.
Montrer que G est commutatif.

V.4 Centre et Commutant ★

[Corrigé]
Soit G un groupe.

1. Montrer que le centre de G définit par :

$$Z(G) = \{a \in G,\ \forall x \in G, ax = xa\}$$

est un sous-groupe de G.

2. Montrer que pour tout $x \in G$, le commutant de x définit par :

$$\mathcal{C}(x) = \{a \in G,\ ax = xa\}$$

est un sous groupe de G.

V.5 Théorème de Dixon ★★★★

[Corrigé]
Soit G un groupe fini non commutatif. Montrer que la probabilité que deux éléments choisis au hasard dans G commutent est inférieure à $\frac{5}{8}$.

V.6 Opérations sur les sous-groupes ★★

[Corrigé]
Soient G un groupe et H, K deux sous-groupes de G.

1. Montrer que $H \cap K$ est un sous-groupe de G.
2. Montrer que $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.

V.7 Sous-groupes finis de $\mathbb{U}$ ★★

[Corrigé]

1. Déterminer les sous-groupes finis de $\mathbb{U}$.

On fixe m et n deux entiers naturels.

2. Montrer que $\mathbb{U}_m \subset \mathbb{U}_n \iff m|n$.
3. Montrer que $\mathbb{U}_m \cap \mathbb{U}_n = \mathbb{U}_{m\wedge n}$.
4. Déterminer le sous-groupe engendré par $\mathbb{U}_m \cup \mathbb{U}_n$.

V.8 Groupes quasi-cycliques de Prüfer ★★★

[Corrigé]
Soit p un nombre premier. On pose $G_p = \{z \in \mathbb{C},\ \exists k \in \mathbb{N},\ z^{p^k} = 1\}$.

1. Montrer que G_p est un sous-groupe de $(\mathbb{U}, \times)$.
2. Décrire G_p à l'aide des groupes cycliques $\mathbb{U}_{p^k}$ des racines p^k-ièmes de l'unité.
3. Montrer que les sous-groupes stricts de G_p sont cycliques et qu'aucun d'entre eux n'est maximal pour l'inclusion.

V.9 Sous-groupes de $\mathrm{GL}_n(\mathbb{C})$ cyclique ★★★

[Corrigé]
On désigne par $\mathrm{SL}_n(\mathbb{C})$ l'ensemble des matrices à coefficients complexes dont le déterminant vaut 1.
Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{C})$ tel que $G \cap \mathrm{SL}_n(\mathbb{C}) = \{I_n\}$.
Montrer que G est cyclique.

V.10 Matrices inversibles à coefficients entiers ★★

[Corrigé]
On note $\mathrm{GL}_n(\mathbb{Z})$ l'ensemble des matrices inversibles à coefficients entiers de $\mathcal{M}_n(\mathbb{R})$ dont l'inverse est aussi à coefficients entiers.

1. Montrer que si M est à coefficients dans $\mathbb{Z}$, alors $M \in \mathrm{GL}_n(\mathbb{Z})$ si et seulement si $\det(M) = \pm 1$.
2. Montrer que $\mathrm{GL}_n(\mathbb{Z})$ est un sous groupe de $\mathrm{GL}_n(\mathbb{R})$.

V.11 Sous-groupes de $(\mathbb{Z}, +)$ ★★

[Corrigé]
Soit G un sous-groupe de $\mathbb{Z}$ différent du sous-groupe trivial $\{0\}$.

1. Justifier l'existence de $a = \min G \cap \mathbb{N}^*$.
2. Montrer que $a\mathbb{Z} \subset G$.
3. Montrer que $G = a\mathbb{Z}$.

V.12 Sous-groupes de $(\mathbb{R}, +)$ ★★★

[Corrigé]
Soit G un sous-groupe non trivial de $\mathbb{R}$ i.e $G \neq \{0\}$.

1. Justifier que $G \cap \mathbb{R}_+^*$ possède une borne inférieure que l'on notera a.
2. On suppose $a > 0$.
   a. On suppose que $a \notin G$. Justifier l'existence de deux éléments distincts x et y de G appartenant à l'intervalle $]a, 2a[$.
   b. Aboutir à une contradiction pour en déduire que a est dans G.
   c. Montrer que $G = a\mathbb{Z}$
3. On suppose que $a = 0$.
   Montrer que G est dense dans $\mathbb{R}$.

V.12.1 Fonction (multi)périodique ★★★

Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ continue, 1-périodique et π-périodique.
Montrer que f est constante.

V.12.2 $\cos(\mathbb{N})$ ★★★

Montrer que $\{\cos(n), n \in \mathbb{N}\}$ est dense dans $[-1, 1]$.

V.12.3 Valeur d'adhérence du cercle unité ★★★

Soit $z \in \mathbb{U}$. Montrer que 1 est une valeur d'adhérence de la suite $(z^n)_{n\in\mathbb{N}}$.

V.13 Sous-groupes distingué

[Corrigé]
Soit G un groupe
On dit que H est un sous-groupe distingué dans G quand H est un sous groupe de G et

$$\forall g \in G, \forall h \in H, ghg^{-1} \in H$$

.

1. Montrer que le centre de G (défini à V.4) est distingué dans G.
2. Soit f un morphisme de groupe de G dans G'.
   Montrer que $\mathrm{Ker}(f)$ est distingué dans G.

V.14 Nature d'une suite

[Corrigé]

1. Soit $x \in \mathbb{R}\backslash\mathbb{Q}$. Montrer qu'il existe une infinité de couples $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ tels que,
$$\left|x - \frac{p}{q}\right| < \frac{1}{q^2}$$

2. Montrer que la suite de terme général $u_n = \ddots \frac{1}{n \sin n}$ diverge.

V.15 Une relation utile sur les morphismes de groupes

[Corrigé]
Soit G un groupe fini et G' un groupe. Soit $f : G \to G'$ un morphisme de groupe.
Montrer que $|G| = |\mathrm{Ker}(f)| \times |\mathrm{Im}(f)|$.

V.16 Automorphisme d'inversion ★

[Corrigé]
Soit G un groupe. Montrer que $f : \left\{ \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x^{-1} \end{array} \right.$ est un automorphisme si et seulement si G est commutatif.

V.17 Automorphismes intérieurs ★

[Corrigé]
Soit G un groupe. On définit pour un élément $a \in G$ l'application :
$$\varphi_a : \left\{ \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & axa^{-1} \end{array} \right.$$

1. Soit $a \in G$. Montrer que φ_a est un automorphisme de G.
2. On pose $\mathfrak{J}(G) = \{\varphi_a, a \in G\}$. Montrer que $\mathfrak{J}(G)$ est un sous-groupe de $(\mathrm{Aut}(G), \circ)$.

V.18 Endomorphismes continus de $\mathbb{R}$ ★★

[Corrigé]
Montrer que les endomorphismes de groupe de $(\mathbb{R}, +)$ continus sont les homothéties i.e les applications $x \mapsto \lambda x$ avec $\lambda \in \mathbb{R}$.

V.19 Morphismes de $\mathbb{Q}$ dans $\mathbb{Z}$ ★

[Corrigé]
Déterminer les morphismes de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.

V.20 Morphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$

[Corrigé]
Soient $m, n \in \mathbb{N}^*$. Déterminer les morphismes de groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ dans $(\mathbb{Z}/m\mathbb{Z}, +)$.

V.21 Morphismes de $\mathrm{GL}_n(\mathbb{R})$ dans $\mathbb{Z}/m\mathbb{Z}$ ★★★★★

[Corrigé]
Soient $m, n \in \mathbb{N}^*$. Déterminer les morphismes de $(\mathrm{GL}_n(\mathbb{R}), \times)$ dans $(\mathbb{Z}/m\mathbb{Z}, +)$.

V.22 Caractères algébriques de $\mathrm{GL}_n(\mathbb{K})$

[Corrigé]
Soit $\chi : \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^*$ un morphisme de groupe polynomial.
Montrer que χ est une puissance du déterminant.

V.23 Quasi-morphisme ★★★

[Corrigé]
Soient G un groupe, $\delta > 0$ et $f : G \to \mathbb{C}$ non bornée telle que

$$\forall (x, y) \in G^2,\ |f(xy) - f(x)f(y)| \leq \delta$$

1. Montrer que f ne s'annule pas.
2. Soit $(z_n) \in G^{\mathbb{N}}$ telle que $(|f(z_n)|)_{n\in\mathbb{N}}$ diverge vers $+\infty$. Pour x fixé, exprimer $f(x)$ à l'aide de $(z^n)_{n\in\mathbb{N}}$.
3. En déduire que f est un morphisme.

V.24 Morphisme de $\mathbb{Z}^{\mathbb{N}}$ presque nul ★★★

[Corrigé]
Soit $\Phi : \mathbb{Z}^{\mathbb{N}} \to \mathbb{Z}$ un morphisme qui s'annule sur les suites presque nulles (i.e qui n'ont qu'un nombre fini de termes non nuls).

1. Soit $(x_n) \in \mathbb{Z}^{\mathbb{N}}$. Montrer qu'il existe deux suites d'entiers (y_n) et (z_n) telles que $\forall n \in \mathbb{N},\ x_n = 2^n y_n + 3^n z_n$.
2. En déduire que Φ est nul.

V.25 Groupes de matrices

[Corrigé]
Soit G une partie de $\mathcal{M}_n(\mathbb{K})$ tel que $(G, \times)$ est un groupe non trivial.
Montrer qu'il existe $r \in [\![1; n]\!]$ tel que G soit isomorphe à un sous-groupe de $\mathrm{GL}_r(\mathbb{K})$.

V.26 Caractérisation de la finitude d'un groupe par ses sous-groupes ★★★

[Corrigé]
Soit G un groupe. Montrer que G est fini si et seulement si l'ensemble de ses sous-groupes est fini.

V.27 Sous-groupe des éléments d'ordre fini ★★★★

[Corrigé]
Soit G un groupe et E l'ensemble des éléments d'ordre fini de G.
Démontrer que si E est fini alors E est un sous-groupe de G.
On pourra considérer le sous-groupe H engendré par E.

V.28 Relations d'équivalence naturelles sur les groupes ★

[Corrigé]
Soit H un sous-groupe d'un groupe G. On définit trois relations binaires $\sim,\ \sim_g,\ \sim_d$ sur G de la manière suivante :

— $\forall (x, y) \in G^2,\ x \sim y \iff \exists h \in H,\ y = h^{-1}xh$
— $\forall (x, y) \in G^2,\ x \sim_g y \iff \exists h \in H,\ y = hx$
— $\forall (x, y) \in G^2,\ x \sim_d y \iff \exists h \in H,\ y = xh$

Montrer que $\sim,\ \sim_g,\ \sim_d$ sont des relations d'équivalence sur G.

V.29 Théorème de Lagrange ★★★ (HP)

[Corrigé]
Soit G un groupe commutatif fini. Montrer que l'ordre d'un sous-groupe de G divise l'ordre de G.

V.30 Un cas particulier du lemme de Cauchy ★★★★ (HP)

[Corrigé]

1. Soit $(G, *)$ un groupe d'élément neutre e tel que $\forall x \in G,\ x * x = e$.
   a. Montrer que G est commutatif.
   b. On suppose G d'ordre fini. Montrer que $|G|$ est une puissance de 2.
   Indication : Montrer que l'on peut munir G d'une structure de $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel.
2. Soit G un groupe de cardinal $2p$ avec p un nombre premier différent de 2. Montrer que G possède un élément d'ordre p.

V.31 Groupe d'ordre premier ★

[Corrigé]
Montrer que tout groupe d'ordre premier est cyclique.

V.31.1 Plus petit groupe non commutatif ★★★

1. Montrer qu'un groupe cyclique est commutatif.
2. Quel est le plus petit entier n tel qu'il existe un groupe d'ordre n non commutatif ?

V.32 Sous-groupe d'un groupe cyclique ★★★

[Corrigé]
Soit G un groupe cyclique d'ordre $n \in \mathbb{N}^*$. Montrer que pour tout diviseur positif d de n, il existe un unique sous-groupe de G d'ordre d et en déduire que les sous-groupes d'un groupe cyclique sont cycliques.

V.33 Exposant d'un groupe abélien fini ★★★★ (HP)

[Corrigé]
Soit G un groupe abélien fini. Pour tout $x \in G$, on note $O(x)$ l'ordre de x.

1. Soit $(x,y) \in G^2$ tel que $O(x) \wedge O(y) = 1$. Montrer que $O(xy) = O(x)O(y)$. Dans le cas général, a-t-on $O(xy) = \text{ppcm}(O(x), O(y))$?
2. Soit $(m,n) \in (\mathbb{N}^*)^2$. Montrer l'existence de $(m',n') \in (\mathbb{N}^*)^2$ tel que $m'|m$, $n'|n$, $\text{pgcd}(m',n') = 1$ et $\text{ppcm}(m,n) = m'n'$.
3. Montrer qu'il existe $z \in G$ tel que $O(z)$ soit le ppcm des ordres des éléments de G (ce ppcm est appelé l'exposant du groupe G)
4. Soient $\mathbb{K}$ un corps commutatif et G un sous-groupe fini du groupe multiplicatif $\mathbb{K}^*$. Démontrer que G est cyclique.
On admettra qu'un polynôme à coefficients dans $\mathbb{K}$ admet toujours moins de racines que son degre

V.34 Un groupe d'inversible non cyclique

[Corrigé]
Soit $n \geq 3$ un entier.

1. Soit a un entier impair. Montrer que $a^{2^{n-2}} \equiv 1[2^n]$.
2. En déduire que le groupe des inversibles de $\mathbb{Z}/2^n\mathbb{Z}$, $(\mathbb{Z}/2^n\mathbb{Z})^\times$ n'est pas cyclique.

V.35 Ordre dans un groupe de cardinal pair

[Corrigé]
Soit G un groupe de cardinal $2n$.

1. Démontrer que la relation binaire $\mathcal{R}$ définie sur G par :
$$x\mathcal{R}y \iff (x = y \text{ ou } x = y^{-1})$$
est une relation d'équivalence sur G.
2. En déduire que G admet un élément d'ordre deux.

V.36 Ordre dans $\mathbb{Z}/n\mathbb{Z}$ ★★

[Corrigé]
Soit $(k,n) \in \mathbb{Z} \times \mathbb{N}^*$. On note d l'ordre de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$.
Montrer que $d = \dfrac{n}{n \wedge k}$.

V.37 Passage par les groupes

[Corrigé]
Le but de cet exercice est de montrer qu'il n'existe pas d'entier $n \geq 2$ tel que $n|2^n - 1$. On raisonne par l'absurde et on note p le plus petit diviseur premier d'un tel entier n. On note aussi m la classe de 2 dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

1. Montrer que $m|p-1$.
2. Montrer que $m|n$.
3. Conclure.

V.38 Groupe infini non monogène ★

[Corrigé]
Donner un exemple de groupe infini non monogène.

V.39 Groupe non cyclique ★★

[Corrigé]
Soit $(n,m) \in (\mathbb{N}^*)^2$. Montrer que $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +)$ est cyclique si et seulement si $m \wedge n = 1$.

V.40 Ordre dans le groupe symétrique ★★

[Corrigé]
Soit $n \in \mathbb{N}^*$. Déterminer l'ordre de $\sigma \in \mathcal{S}_n$ en fonction de sa décomposition en produit de cycles à supports disjoints.

V.41 Sous-groupe engendré par les nombres premiers

[Corrigé]
Déterminer le sous-groupe engendré par l'ensemble $\mathcal{P}$ des nombres premiers dans $(\mathbb{C}^*, \times)$.

V.42 Sous-groupe engendré par le complémentaire d'un sous-groupe

[Corrigé]
Soit H un sous-groupe strict d'un groupe G.
Déterminer le sous-groupe engendré par le complémentaire de H dans G.

V.43 Partie génératrice

[Corrigé]
Montrer que tout groupe fini G de cardinal $n \geq 2$ possède une partie génératrice constitué d'au plus $\log_2(n)$ éléments.

V.44 Groupe alterné ★★★

[Corrigé]
Soit $n \geq 3$.
On note $\mathcal{A}_n$ l'ensemble des permutations de $\mathcal{S}_n$ de signature 1.

1. Montrer que $\mathcal{A}_n$ est un sous-groupe de $\mathcal{S}_n$.
2. Montrer que $\mathcal{A}_n$ est engendré par les 3-cycles.

V.45 Cardinal minimal d'une famille de transpositions engendrant $\mathcal{S}_n$ ★★★

[Corrigé]
Soit $n \in \mathbb{N}^*$. On note $(e_1, \dots, e_n)$ la base canonique de $\mathbb{R}^n$ et pour $i \in [\![2; n]\!]$ on note $t_i = (1, i)$. Enfin pour tout $s \in \mathcal{S}_n$ on définit $u_s \in \mathcal{L}(\mathbb{R}^n)$ par $\forall i \in [\![1; n]\!],\ u(e_i) = e_{s(i)}$.

1. Montrer que $(t_2, \dots, t_n)$ engendre $\mathcal{S}_n$.
2. Interpréter géométriquement u_s lorsque s est une transposition.
3. Soit $s = (1, \dots, n)$. On suppose que s est la composée de p transpositions. Montrer que $p \geq n - 1$.
4. Quel est le cardinal minimal d'une famille de transposition génératrice de $\mathcal{S}_n$?

V.46 Partie génératrice de $\mathcal{O}(E)$ ★★★★

[Corrigé]
Soit E un espace euclidien. Montrer que $\mathcal{O}(E)$ est engendré par les réflexions.

V.47 Groupe dans un plan euclidien ★★★

[Corrigé]

1. Déterminer les sous-groupes finis de $\mathrm{SO}(E)$.
2. Caractériser les sous-groupes finis de $\mathcal{O}(E)$.
3. Soit G un sous-groupe fini de $\mathrm{GL}(E)$. Déterminer un produit scalaire pour lequel tous les éléments de G sont des endomorphismes orthogonaux.

V.48 Matrices de permutation ★

[Corrigé]
Pour $\sigma \in \mathcal{S}_n$ on pose $P_\sigma = (\delta_{i,\sigma(j)})_{1 \leq i,j \leq n}$ et on définit $\mathcal{P}_n = \{P_\sigma,\ \sigma \in S_n\}$ l'ensemble

des matrices de permutation d'ordre n. $\delta_{i,j}$ représente le symbole de Kronecker, $\delta_{i,j} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$.

1. Montrer que $f : \left\{ \begin{array}{ccc} \mathcal{S}_n & \longrightarrow & \mathcal{P}_n \\ \sigma & \longmapsto & P_\sigma \end{array} \right.$ est un isomorphisme de groupes.
2. Soit $\sigma \in \mathcal{S}_n$. Que vaut $P_\sigma^\top$?
3. Montrer que $\forall \sigma \in \mathcal{S}_n,\ \det P_\sigma = \varepsilon(\sigma)$.

V.49 Groupe dérivé ★★★★

[Corrigé]

Soit G un groupe. On note D le sous-groupe (dit dérivé) de G engendré par les éléments de la forme $xyx^{-1}y^{-1}$ (avec $x, y \in G$) et C celui engendré par les éléments de la forme x^2 ($x \in G$).

1. Montrer que $D \subset C$.
2. On suppose que G est engendré par les éléments de G qui vérifient $x = x^{-1}$. Montrer que $D = C$.
3. a. Montrer que toute matrice de $\mathrm{SO}_2(\mathbb{R})$ peut s'écrire comme un produit de deux symétries. Y a-t-il unicité ?
   b. Montrer que $\mathcal{O}_2(\mathbb{Q}) = \mathcal{M}_2(\mathbb{Q}) \cap \mathcal{O}_2(\mathbb{R})$ est un groupe puis que $\mathrm{SO}_2(\mathbb{Q}) = \{M \in \mathcal{O}_2(\mathbb{Q}),\ \det(M) = 1\}$ est un sous-groupe commutatif de $\mathcal{O}_2(\mathbb{Q})$. Démontrer que le sous-groupe dérivé de $\mathcal{O}_2(\mathbb{Q})$ est un sous-groupe strict de $\mathrm{SO}_2(\mathbb{Q})$.

V.50 Sous-groupe discret de $\mathbb{C}$ et de $\mathrm{SL}_2(\mathbb{R})$ ★★★★★

[Corrigé]

On dit qu'une partie A d'un espace vectoriel normée est discrète si en tout point x de A on peut trouver un voisinage qui ne contient pas d'élément de A, hormis x. On s'intéresse dans cet exercice aux sous-groupes discrets de $(\mathbb{C}, +)$ et de $(\mathrm{SL}_2(\mathbb{R}), \times)$.

1. Donner des exemples de sous-groupes discrets de $\mathbb{C}$ et de $\mathrm{SL}_2(\mathbb{R})$.
2. Soit Γ un sous-groupe discret non trivial de $(\mathbb{C}, +)$ et $\lambda \in \mathbb{C}^*$ vérifiant $\lambda\Gamma = \Gamma$. Montrer que $\lambda^4 = 1$ ou $\lambda^6 = 1$.
3. Soient $\lambda \in \mathbb{R}^*$ et Γ le sous-groupe engendré par $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$. A quelle condition sur λ le sous-groupe Γ est-il discret ?

VI

Anneaux et corps

Pour $(A, +, \times)$ un anneau on désignera par 0_A ou simplement 0 son neutre additif et par 1_A ou simplement 1 son neutre multiplicatif.

VI.1 Centre d'un anneau ★ (HP)

[Corrigé]
Soit $(A, +, \times)$ un anneau. On pose $Z(A) = \{x \in A,\ \forall a \in A,\ ax = xa\}$.

1. Montrer que $Z(A)$ est un sous-anneau commutatif de A.
2. On suppose que $Z(A)$ est un corps. Montrer que $(A, +, \times, \cdot)$ où $\cdot$ est la loi $\times$ est une $Z(A)$-algèbre unitaire, associative et commutative.

VI.2 Calcul d'un inverse ★★★

[Corrigé]
Soient A un anneau et $(a, b) \in A^2$ tel que $1 - ab$ est inversible.

1. On suppose que ab est nilpotent.
   Montrer que ba est nilpotent puis que $1 - ba$ est inversible.
2. Montrer que $1 - ba$ est inversible.

VI.3 Anneau de Boole ★★

[Corrigé]
Soit E un ensemble non vide. Pour $A, B \in \mathcal{P}(E)$ on définit la différence symétrique de A

par B par $A\Delta B = (A\backslash B) \cup (B\backslash A)$.

1. Montrer que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif.
2. Quels sont les éléments de $\mathcal{P}(E)$ inversibles pour la loi $\cap$?
3. l'anneau $(\mathcal{P}(E), \Delta, \cap)$ est-t-il intègre ?

VI.3.1 L'anneau de Boole est principal ★★★

Montrer que les idéaux de $(\mathcal{P}(E), \Delta, \cap)$ sont de la forme $\mathcal{P}(F)$ avec $F \subset E$.

VI.4 Condition suffisante pour qu'un anneau soit commutatif ★★★

[Corrigé]
Soit $(A, +, \times)$ un anneau.

1. On suppose que $\forall x \in A,\ x^2 = x$
   Montrer que A est commutatif.
2. On suppose que $\forall x \in A, x^3 = x$
   a. Déterminer les éléments nilpotents de A.
   b. Soient $e \in A$ tel que $e^2 = e$, $a \in A$ et $b = ea(1-e)$.
   Calculer b^2 et en déduire que $ea = ae$.
   En déduire que pour tout $x \in A$, $x^2 \in Z(A)$ où $Z(A)$ désigne le centre de $(A, +, \times)$ (cf. VI.1).
   c. Montrer que pour tout $x \in A$, $(2x, 3x) \in Z(A)^2$ et en déduire que A est commutatif.

De manière plus générale, un théorème dû à Jacobson énonce que si pour tout $x \in A$ il existe $n \in \mathbb{N}$ tel que $x^n = x$ alors A est commutatif.

VI.5 Anneaux commutatifs ou anti-commutatifs ★★★★

[Corrigé]
Un pseudo-anneau est un triplet $(A, +, \times)$ qui vérifie tous les axiomes de la structure d'anneau sauf l'existence de l'élément neutre unité.
On se donne A un pseudo-anneau tel que $\forall x, y \in A, xy \in \{yx, -yx\}$. Montrer que A est commutatif ou anti-commutatif.
Que dire si A est un anneau ?

VI.6 Anneau régulier ★★★★

[Corrigé]
On dit qu'un anneau A est *régulier* lorsque $\forall a \in A, \exists u \in A,\ aua = a$.

1. $(\mathbb{Z}, +, \times)$ est-t-il régulier ?
2. Un corps est-t-il régulier ?
3. a. Montrer que si A et B sont deux anneaux réguliers alors l'anneau produit $A \times B$ est régulier.
   b. Soit $n \in \mathbb{N}$. Déterminer une condition nécessaire et suffisante pour que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ soit régulier.
4. a. Soit E un espace vectoriel. Montrer que $(\mathcal{L}(E), +, \circ)$ est régulier.
   b. Soit $n \in \mathbb{N}^*$. On note A la matrice de $\mathcal{M}_n(\mathbb{K})$ n'ayant que des 0, sauf sur sa sur-diagonale où il n'y a que des 1.
   Exhiber une matrice $U \in \mathcal{M}_n(\mathbb{K})$ telle que $AUA = A$.
5. Montrer que le centre d'un anneau régulier est régulier (cf. VI.1).

VI.7 Anneau intègre fini ★

[Corrigé]
Montrer qu'un anneau intègre fini est un corps.

VI.8 Anneau principal (1) ★★★

[Corrigé]
Soit $(A, +, \times)$ un anneau commutatif. On dit qu'un idéal I de A est *principal* lorsqu'il existe $x \in A$ tel que $I = xA$. Lorsque tous les idéaux de A sont principaux, on dit que A est un anneau principal.

1. Montrer que $(\mathbb{Q}, +, \times)$ est un anneau principal.
2. Montrer que $(\mathbb{Z}, +, \times)$ est un anneau principal.
3. Montrer que $(\mathbb{D}, +, \times)$ est un anneau principal.
4. Soit $n \in \mathbb{N}^*$. Montrer que $(\mathbb{Z}/n\mathbb{Z}, +)$ est principal.

VI.9 Anneau principal (2) ★★★ (HP)

[Corrigé]
Soit $(A, +, \times)$ un anneau commutatif. On dit qu'un idéal I de A est *principal* lorsqu'il existe $x \in A$ tel que $I = xA$. Lorsque tous les idéaux de A sont principaux, on dit que A est un anneau principal.

1. $(\mathbb{Z}, +, \times)$ est-il principal ?
2. $(\mathbb{Z}[X], +, \times)$ est-il principal ?
3. Soit A un anneau commutatif. A quelle condition $A[X]$ est-il principal ?
   On admettra que l'on peut définir une notion de degré dans $A[X]$ analogue à celle de $\mathbb{C}[X]$ ou de $\mathbb{R}[X]$.

VI.10 Anneau euclidien ★★

[Corrigé]
Soit $(A, +, \times)$ un anneau intègre.
On dit que A est un anneau euclidien lorsqu'il existe une application $\varphi : A\backslash\{0_A\} \longrightarrow \mathbb{N}$ telle que pour $a \in A$ et $b \in A\backslash\{0_A\}$, il existe $(q, r) \in A^2$ tel que :

$$a = bq + r \text{ et } (r = 0_A \text{ ou } \varphi(r) < \varphi(b))$$

1. Donner des exemples d'anneaux euclidiens.
2. Montrer qu'un anneau euclidien est principal (cf. VI.8).

VI.11 Entiers de Gauss

[Corrigé]
On note $\mathbb{Z}[i] = \{a + ib,\ (a, b) \in \mathbb{Z}^2\}$.

VI.11.1 Structure et inversibles de $\mathbb{Z}[i]$ ★★

1. Montrer que $(\mathbb{Z}[i], +, \times)$ est un anneau commutatif intègre.
2. Déterminer $\mathbb{Z}[i]^\times$, l'ensemble des inversibles de $\mathbb{Z}[i]$.

On admet ses résultats comme connus dans les exercices qui suivent et on pose pour tous $x \in \mathbb{Z}[i],\ N(x) = x\overline{x}$.

VI.11.2 $\mathbb{Z}[i]$ est euclidien ★★★

Démontrer que :

$$\forall (x, y) \in \mathbb{Z}[i] \times \mathbb{Z}[i]\backslash\{0\},\ \exists (q, r) \in \mathbb{Z}[i],\ x = qy + r \wedge N(r) < N(a)$$

En déduire que tous les idéaux de $\mathbb{Z}[i]$ sont de la forme $x\mathbb{Z}[i]$ avec $x \in \mathbb{Z}[i]$.

VI.11.3 Une somme ★★★★

Soit $(n, k) \in \mathbb{N} \times \mathbb{N}^*$.
Montrer que $\dfrac{1}{4} \displaystyle\sum_{\substack{x \in \mathbb{Z}[i] \\ N(x) = n}} x^k \in \mathbb{Z}$.

VI.11.4 Irréductibles de $\mathbb{Z}[i]$ ★★★★

1. Soit $a \in \mathbb{Z}[i]$. Montrer que si $N(a)$ est premier alors a est irréductible dans $\mathbb{Z}[i]$, c'est à dire :
   $a \notin \mathbb{Z}[i]^\times \wedge \forall (b,c) \in \mathbb{Z}[i]^2,\ a = bc \implies (b \in \mathbb{Z}[i]^\times \vee c \in \mathbb{Z}[i]^\times)$.
2. Soit p un nombre premier. Montrer l'équivalence des propriétés suivantes :
   (i) p est irréductible dans $\mathbb{Z}[i]$;
   (ii) $p \equiv 3[4]$;
   (iii) il n'existe pas $a \in \mathbb{Z}[i]$ tel que $p = N(a)$.
   On admettra que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si p n'est pas congrus à 3 modulo 4.
3. En déduire tous les irréductibles de $\mathbb{Z}[i]$.

VI.12 Anneau Noethérien ★★★★ (HP)

[Corrigé]
Un anneau commutatif $(A, +, \times)$ est dit *noethérien* lorsque tous ses idéaux sont engendrés par un nombre fini d'élément (on dit que ses idéaux sont de types finis).
Soit A un anneau commutatif. Montrer que les trois propositions suivantes sont équivalentes :

(i) A est noethérien ;
(ii) toute suite croissante (pour l'inclusion) d'idéaux de A stationne ;
(iii) Tout ensemble non vide d'idéaux de A admet un élément maximal pour l'inclusion.

Remarque : l'appellation d'anneau noethérien provient de la mathématicienne Emmy Noether qui s'est intéressée aux propriétés de tels anneaux. Son influence sur les sciences s'étend aussi à la physique notamment par le théorème de Noether qui explique le lien fondamental entre la symétrie et les lois de conservation.

VI.12.1 $\mathbb{Z}$ et $\mathbb{K}[X]$ sont noethériens ★★

1. Montrer que toute suite croissante d'idéaux de $\mathbb{Z}$ stationne.
2. Montrer que toute suite croissante d'idéaux de $\mathbb{K}[X]$ stationne.

VI.13 Morphismes d'anneaux de fonctions réelles

[Corrigé]
On note $\mathcal{C}(\mathbb{R}, \mathbb{R})$ l'ensemble des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$ et $\mathcal{D}(\mathbb{R}, \mathbb{R})$ celui des fonctions dérivables de $\mathbb{R}$ dans $\mathbb{R}$.
Déterminer les morphismes d'anneaux de $\mathcal{C}(\mathbb{R}, \mathbb{R})$ dans $\mathcal{D}(\mathbb{R}, \mathbb{R})$.
Indication : on pourra montrer qu'un tel morphisme est nécessairement à valeurs dans l'ensemble des fonctions constantes

VI.14 Caractérisation d'un corps par ses idéaux ★★

[Corrigé]
Soit A un anneau non nul.
Montrer que A est un corps si et seulement si ses seuls idéaux sont $\{0_A\}$ et A.

VI.15 Opérations sur les idéaux, idéaux principaux ★★★

[Corrigé]
Soit A un anneau commutatif. On dit qu'un idéal I de A est *principal* s'il existe $x \in A$ tel que $I = xA$.

1. Montrer que si I et J sont deux idéaux de A alors $I + J$ et $I \cap J$ sont aussi des idéaux de A.
2. a. Soit $(a, b) \in \mathbb{Z}^2$. Donner deux entiers c et d tels que $a\mathbb{Z} \cap b\mathbb{Z} = c\mathbb{Z}$ et $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.
   b. Montrer que si I, J et $I + J$ sont des idéaux principaux de A alors $I \cap J$ en est aussi un.

VI.16 Idéal premier ★★

[Corrigé]
Soit A un anneau commutatif. On dit qu'un idéal I de A est *premier* lorsque $A \backslash I$ est stable pour le produit i.e :

$$\forall (x, y) \in A^2,\ xy \in I \implies (x \in I \text{ ou } y \in I)$$

Soit A un anneau commutatif dont tous les idéaux sont premiers. Montrer que A est un corps.

VI.17 Idéal maximal ★★★★

[Corrigé]
Soient A un anneau commutatif et I un idéal de A.
On dit que I est un idéal *maximal* de A lorsqu'il est contenu dans exactement deux idéaux de A, A et lui-même. (Ainsi A n'est pas maximal)

1. Montrer que I est maximal si et seulement si $\forall a \in A \backslash I,\ I + aA = A$.
2. Montrer que tout idéal maximal est premier (cf. VI.16).
3. Donner un exemple d'idéal premier.

4. On note $A = (\mathcal{C}^\infty(\mathbb{R}, \mathbb{R}), +, \times)$. Pour chacun des cas présentés, Vérifier que l'ensemble est un idéal de A et préciser s'il est principal, premier, maximal.
   a. l'ensemble I des fonctions de A qui s'annule en 0.
      On pourra considérer la fonction g définie par $g(x) = \dfrac{f(x)}{x}$ si $x \neq 0$ et $g(0) = f'(0)$.
   b. l'ensemble J des fonctions f de A telle que $\forall k \in \mathbb{N},\ f^{(k)}(0) = 0$.
      On pourra déterminer une fonction de J et montrer qu'elle ne s'annule qu'en 0.

VI.18 Idéaux d'un espace de fonction

[Corrigé]
Soit K une partie compacte d'un espace vectoriel normé. On note $A = \mathcal{C}^0(K, \mathbb{R})$. Pour tout $x \in K$, on note $m_x = \{f \in A,\ f(x) = 0\}$.

1. Montrer que tout idéal propre de A (i.e différent de E.) est contenu dans un m_x.
2. Donner un contre exemple quand K n'est pas compact.

VI.19 Radical d'un idéal ★

[Corrigé]
Soit A un anneau commutatif. Pour tout idéal I de A On note

$$R(I) = \{x \in A,\ \exists n \in \mathbb{N},\ x^n \in I\}$$

L'ensemble $R(I)$ est appelé *radical* de I.

1. Soit I un idéal de A. Montrer que $R(I)$ est un idéal de A qui contient I.
2. Soit I un idéal de A. Montrer que $R(R(I)) = R(I)$.
3. Soient I et J deux idéaux de A. Montrer que $R(I \cap J) = R(I) \cap R(J)$.

VI.20 Nilradical ★★

[Corrigé]
Soit A un anneau commutatif. On appelle *nilradical* de A l'ensemble $\mathcal{N}(A)$ des éléments nilpotents de A.

1. Montrer que le nilradical est un idéal.
2. Soit $n \in \mathbb{N}^*$. Déterminer le nilradical de $\mathbb{Z}/n\mathbb{Z}$.

VI.21 Radical de Jacobson ★★

[Corrigé]
Soit A un anneau commutatif. Un idéal de A est dit *maximal* lorsque qu'il est contenu dans exactement deux idéaux de A, A et lui-même (ainsi A n'est pas maximal).
On note $A^\times$ l'ensemble des inversibles de A et $\mathcal{I}(A)$ l'ensemble des idéaux maximaux de A.
Enfin on pose le radical de Jacobson :

$$J = \bigcap_{I \in \mathcal{I}(A)} I$$

1. Soit I un idéal de A. Montrer que I est maximal si et seulement si $\forall a \in A \backslash I,\ I + aA = A$.
2. Montrer que $x \in J \iff \forall a \in A,\ 1_A - ax \in A^\times$.
   On admettra le théorème de Krull : Dans un anneau commutatif unitaire, tout idéal autre que l'anneau lui-même est contenu dans un idéal maximal.

VI.22 Idéaux de $\mathcal{M}_n(\mathbb{K})$

[Corrigé]
Un sous-groupe J de $(\mathcal{M}_n(\mathbb{K}), +)$ est appelé *idéal à droite* de $\mathcal{M}_n(\mathbb{K})$ lorsque :

$$\forall A \in \mathcal{M}_n(\mathbb{K}),\ \forall M \in J,\ MA \in J$$

Un sous-groupe J de $(\mathcal{M}_n(\mathbb{K}), +)$ est appelé *idéal à gauche* de $\mathcal{M}_n(\mathbb{K})$ lorsque :

$$\forall A \in \mathcal{M}_n(\mathbb{K}),\ \forall M \in J,\ AM \in J$$

Lorsque J est à la fois un idéal à gauche et à droite, on dit que J est un *idéal bilatère*.

VI.22.1 Idéaux bilatère ★★★

Soit J un idéal bilatère de $\mathcal{M}_n(\mathbb{K})$.

1. Montrer que si $I_n \in J$ alors $J = \mathcal{M}_n(\mathbb{K})$.
2. Montrer que si J contient une matrice inversible alors $J = \mathcal{M}_n(\mathbb{K})$.
3. On suppose que J n'est pas réduit à $\{0\}$ et on fixe une matrice $A \in J$ de rang r non nul.
   a. Montrer que $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \in J$
   b. Justifier l'existence de $n - r + 1$ matrices $A_1, \dots, A_{n-r+1}$, toutes équivalentes à A et telles que la somme $A_1 + \cdots + A_{n-r+1}$ est inversible.
4. Que peut-on dire des idéaux bilatères de $\mathcal{M}_n(\mathbb{K})$?

VI.22.2 Idéaux à droite ★★

Soit E un sous-espace vectoriel de $\mathcal{M}_{n,1}(\mathbb{K})$. On pose $J_E = \{M \in \mathcal{M}_n(\mathbb{K}),\ \mathrm{Im}(M) \subset E\}$.

1. Montrer que J_E est un idéal à droite de $\mathcal{M}_n(\mathbb{K})$.
2. Soient $p, q \in [\![1; n]\!]$, $u \in \mathcal{L}(\mathbb{R}^p, \mathbb{R}^n)$ et $v \in \mathcal{L}(\mathbb{R}^q, \mathbb{R}^n)$ tels que l'image de v est contenue dans celle de u. On fixe S un supplémentaire de $\mathrm{Ker}(u)$ dans $\mathbb{R}^p$ et on note $(e_1, \dots, e_q)$ la base canonique de $\mathbb{R}^q$.
   a. Justifier l'existence, pour tout $i \in [\![1; q]\!]$, d'un unique élément $\varepsilon_i \in S$ tel que $u(\varepsilon_i) = v(e_i)$.
   b. En déduire l'existence de $w \in \mathcal{L}(\mathbb{R}^q, \mathbb{R}^p)$ telle que $v = u \circ w$.
   c. Soit $(A, B) \in \mathcal{M}_{n,p}(\mathbb{K}) \times \mathcal{M}_{n,q}\mathbb{K}$ tel que $\mathrm{Im}(B) \subset \mathrm{Im}(A)$.
   Déduire de ce qui précède l'existence d'une matrice $C \in \mathcal{M}_{p,q}(\mathbb{K})$ vérifiant que $B = AC$.
3. Soient A, B et C trois matrices carrées d'ordre n à coefficients dans $\mathbb{K}$ telles que $\mathrm{Im}(C) \subset \mathrm{Im}(A) + \mathrm{Im}(B)$.
   a. On désigne par $D = (A|B)$ la matrice de $\mathcal{M}_{n,2n}\mathbb{K}$ obtenue en juxtaposant les matrices A et B, c'est à dire que les n première colonnes de D sont celles de A et les n dernières sont celles de B.
   Montrer que $\mathrm{Im}(D) = \mathrm{Im}(A) + \mathrm{Im}(B)$
   b. En déduire l'existence de deux matrices $U, V \in \mathcal{M}_n(\mathbb{K})$ vérifiant $C = AU + BV$.
4. Soit J un idéal à droite de $\mathcal{M}_n(\mathbb{K})$.
   a. Montrer que $\exists M_0 \in J,\ \forall M \in J,\ \mathrm{rg}(M) \leq \mathrm{rg}(M_0)$. On note $r = \mathrm{rg}(M_0)$ pour la suite.
   b. Soit $M \in J$ telle que $\mathrm{Im}(M) \not\subset \mathrm{Im}(M_0)$.
   En utilisant le sous-espace vectoriel $\mathrm{Im}(M) + \mathrm{Im}(M_0)$, montrer l'existence d'un élément de J de rang strictement supérieur à r.
   c. Montrer que $J = J_{M_0}$.
5. Quels sont les idéaux à droite de $\mathcal{M}_n(\mathbb{K})$?

VI.22.3 Idéaux à gauche ★★

Soit E un sous-espace vectoriel de $\mathcal{M}_{n,1}(\mathbb{K})$. On pose $J^E = \{M \in \mathcal{M}_n(\mathbb{K}),\ E \subset \mathrm{Ker}(M)\}$.

1. Montrer que J^E est un idéal à gauche de $\mathcal{M}_n(\mathbb{K})$.
2. Soient $p, q \in [\![1; n]\!]$, $u \in \mathcal{L}(\mathbb{R}^n, \mathbb{R}^p)$ et $v \in \mathcal{L}(\mathbb{R}^q, \mathbb{R}^p)$ tels que $\mathrm{Ker}(u) \subset \mathrm{Ker}(v)$. On note $(e_1, \dots, e_n)$ une base de $\mathbb{R}^n$ telle que $(e_{r+1}, \dots, e_n)$ soit une base de $\mathrm{Ker}(u)$.
   a. Montrer que $(u(e_1), \dots, u(e_r))$ est une famille libre de $\mathbb{R}^p$.
   b. Montrer qu'il existe $w \in \mathcal{L}(\mathbb{R}^p, \mathbb{R}^q)$ telle $v = w \circ u$.
   c. Soit $(A, B) \in \mathcal{M}_{p,n}\mathbb{K} \times \mathcal{M}_{q,n}\mathbb{K}$ tel que $\mathrm{Ker}(A) \subset \mathrm{Ker}(B)$.
   Déduire de ce qui précède l'existence d'une matrice $C \in \mathcal{M}_{q,p}\mathbb{K}$ vérifiant $B = CA$.

3. Soient A, B et C trois matrices carrées d'ordre n à coefficients dans $\mathbb{K}$ telles que $\text{Ker}(A) \cap \text{Ker}(B) \subset \text{Ker}(C)$.
   Montrer qu'il existe deux matrices $U, V \in \mathcal{M}_n(\mathbb{K})$ telles que $C = UA + VB$.
4. Quels sont les idéaux à gauche de $\mathcal{M}_n(\mathbb{K})$?

VI.23 Caractéristique d'un anneau ★★ (HP)

[Corrigé]
Soit A un anneau.

1. Montrer que l'application $\varphi : \mathbb{Z} \longmapsto A$ définie par $\varphi(k) = k.1_A$ est un morphisme d'anneaux.
2. Justifier qu'il existe $n \in \mathbb{N}$ tel que $\ker(\varphi) = n\mathbb{Z}$.
   Cet entier est appelé caractéristique de l'anneau A.
3. Montrer que la caractéristique d'un anneau intègre est nulle ou égale à un nombre premier.
4. Soit K un corps fini de caractéristique p. Montrer que p est un nombre premier puis qu'on peut munir K d'une structure de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. En déduire qu'il existe $n \in \mathbb{N}$ tel que $\text{Card}(K) = p^n$.

VI.24 Anneau intègre ★★ (HP)

[Corrigé]

1. Montrer qu'un corps est intègre.
2. Donner un exemple d'anneau intègre qui n'est pas un corps.
3. Montrer que pour A un anneau commutatif, $A[X]$ est intègre si et seulement si A l'est.

VI.25 Sous-corps minimal de $\mathbb{C}$ ★

[Corrigé]
Démontrer l'existence et déterminer le sous-corps de $\mathbb{C}$ minimal au sens de l'inclusion.

VI.26 Corps d'Attila

[Corrigé]
On note A la matrice de $\mathcal{M}_n(\mathbb{K})$ qui n'est composée que de 1.

1. Montrer que $(\text{Vect}(A), +, \times)$ est un corps.
2. Justifier que $(\text{Vect}(A)\backslash\{0\}, \times)$ est un groupe et expliciter son élément neutre.

VI.27 Endomorphisme de corps de $\mathbb{R}$ ★★

[Corrigé]
Soit f un endomorphisme de corps de $\mathbb{R}$.

1. Montrer que $f_{|\mathbb{Q}} = \mathrm{Id}_{\mathbb{Q}}$.
2. Montrer que f est croissant.
3. Montrer que $f = \mathrm{Id}_{\mathbb{R}}$.

VI.28 Automorphismes de $\mathbb{Q}[\sqrt{2}]$ ★★★

[Corrigé]
On note $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2},\ (a,b) \in \mathbb{Q}^2\}$.
Montrer que $\mathbb{Q}[\sqrt{2}]$ est un sous-corps de $\mathbb{C}$ et en déterminer tous les automorphismes.

VI.29 Algèbre des quaternions

[Corrigé]
On se place dans $\mathcal{M}_2(\mathbb{C})$ et on pose les matrices

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad K = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

On note $\mathbb{H} = \mathrm{Vect}(I_2, I, J, K)$.

1. Montrer que $I^2 = J^2 = K^2 = IJK = -I_2$.
2. Montrer que $\mathbb{H}$ est une sous-algèbre non commutative de $\mathcal{M}_2(\mathbb{C})$. Quelle est sa dimension ?

Pour un élément $Q = aI_2 + bI + cJ + dK$ on définit son *conjugué quaternionique* $\overline{Q} = aI_2 - bI - cJ - dK$ et on pose $\|Q\| = \sqrt{Q\overline{Q}}$.

3. Montrer que $\|\cdot\|$ définit une norme sur $\mathbb{H}$.
4. Montrer que $\forall (Q_1, Q_2) \in \mathbb{H}^2$, $\overline{Q_1 Q_2} = \overline{Q}_2 \times \overline{Q}_1$. L'application $Q \mapsto \overline{Q}$ est-elle $\mathbb{R}$-linéaire ? $\mathbb{C}$-linéaire ?
5. Montrer que $(\mathbb{H}, +, \times)$ est un corps.
6. Déterminer le centre de $\mathbb{H}$ (cf. VI.1).

VI.30 Une définition de $\mathbb{C}$ ★★

[Corrigé]

1. Montrer que l'application $\Phi : \begin{cases} \mathbb{C} & \longrightarrow & \mathcal{M}_2(\mathbb{R}) \\ z & \longmapsto & \begin{pmatrix} \Re(z) & -\Im(z) \\ \Im(z) & \Re(z) \end{pmatrix} \end{cases}$ est un morphisme d'algèbre injectif.
2. Pour $\theta \in \mathbb{R}$ on pose $A_\theta = \begin{pmatrix} 0 & -\theta \\ \theta & 0 \end{pmatrix}$. Calculer $\exp(A_\theta)$.

VI.31 $\mathbb{R}$-algèbre commutative intègre de dimension finie ★★★★

[Corrigé]
Soit $\mathbb{K}$ une $\mathbb{R}$-algèbre commutative intègre de dimension finie $n \geq 2$.

1. Soit $a \in \mathbb{K}\backslash\{0\}$. Montrer que $f : x \mapsto ax$ est un automorphisme et en déduire que a est inversible.
2. Soit $a \in \mathbb{K}\backslash\mathbb{R}$. Montrer que $(1, a)$ est libre et que $(1, a, a^2)$ est liée.
3. Montrer l'existence de $i \in \mathbb{K}$ tel que $i^2 = -1_{\mathbb{K}}$, puis que $\mathbb{K}$ est isomorphe à $\mathbb{C}$ en tant que $\mathbb{R}$-algèbre.

VI.32 Théorie algébrique des corps ★★★★ (HP)

[Corrigé]
Soit $\mathbb{L}$ un corps commutatif et $\mathbb{K}$ un sous corps quelconque de $\mathbb{L}$. On dit que $a \in \mathbb{L}$ est *algébrique sur* $\mathbb{K}$ s'il existe un polynôme $P \in \mathbb{K}[X]$ non nul qui annule a.

1. Montrer que $\mathbb{K}[X]$ est un anneau principal, c'est à dire que tous ses idéaux sont de la forme $P\mathbb{K}[X]$ avec $P \in \mathbb{K}[X]$.
2. Soit $a \in \mathbb{L}$ algébrique sur $\mathbb{K}$. Montrer l'existence d'un unique polynôme unitaire $\mu \in \mathbb{K}[X]$ tel que
$$\forall P \in \mathbb{K}[X],\ P(a) = 0 \implies \mu | P$$
Vérifier que μ est irréductible et que l'ensemble $\mathbb{K}[a] = \{P(a),\ P \in \mathbb{K}[X]\}$ est à la fois un $\mathbb{K}$-espace vectoriel de dimension $\deg \mu$ et un sous-corps de $\mathbb{L}$. (μ est appelé *polynôme minimal* de a sur $\mathbb{K}$)
3. On dit qu'un nombre complexe a est *algébrique* s'il est algébrique sur le corps $\mathbb{Q}$. Démontrer que $a = \sqrt{2} + \sqrt[3]{2}$ est algébrique et déterminer son polynôme minimal.
On pourra utiliser la relation de multiplicativité des degrés (cf. I.1).

VI.33 Famille $\mathbb{Q}$-libre ★★★★ (HP)

[Corrigé]
Dans tout cet exercice on travaille dans $\mathbb{C}$ munit de sa structure de $\mathbb{Q}$-espace vectoriel.

Soient $p_1, \dots, p_n$ des nombres premiers distincts. Pour toute famille $\mathcal{F} = (z_1, \dots, z_p)$ d'éléments de $\mathbb{C}$ on note $\mathbb{Q}(z_1, \dots, z_p)$ le plus petit sous-corps de $\mathbb{C}$ qui contient $\mathbb{Q}$ et $\mathcal{F}$. Pour $\alpha \in \mathbb{C}$ on note $m_\alpha : x \in \mathbb{C} \mapsto \alpha x$ et enfin, si α est algébrique on note π_α son polynôme minimal (cf. VI.32). On fixe dans tout l'exercice α un nombre algébrique.

1. Montrer que $\mathbb{Q}(\alpha)$ est un $\mathbb{Q}$-espace vectoriel de dimension finie dont on précisera la dimension en fonction de π_α. Montrer que m_α est un endomorphisme de $\mathbb{Q}(\alpha)$.
2. Montrer que si $d \in \mathbb{N}$ n'est pas le carré d'un entier alors $\mathbb{Q}(\sqrt{d})$ est un $\mathbb{Q}$-espace vectoriel de dimension 2 et en donner une base.
3. Montrer que $\pi_{m_\alpha} = \pi_\alpha$ et en déduire que χ_{m_α} est une puissance de π_α.
4. Soient $1 \leq i \neq j \leq n$. Montrer $\mathrm{Tr}(m_{\sqrt{p_i p_j}}) = 0$ puis que la matrice $(\mathrm{Tr}(m_{\sqrt{p_i p_j}}))_{1 \leq i,j \leq n}$ est inversible.
5. En déduire que $(\sqrt{p}_1, \dots, \sqrt{p}_n)$ est libre dans $\mathbb{Q}$.

VI.34 Corps des nombres algébriques ★★★★

[Corrigé]

On note $\mathbb{A} = \{z \in \mathbb{C} \mid \exists P \in \mathbb{Q}[X] \backslash \{0\},\ P(z) = 0\}$ l'ensemble des nombres algébriques.

Montrer que $(\mathbb{A}, +, \times)$ est un corps.
Indication : pour la stabilité par somme et par produit on pourra poser pour $(x, y) \in \mathbb{A}^2$,

$$V = \left(1\ x\ x^2\ \cdots\ x^{n-1}\ y\ xy\ x^2y\ \cdots\ x^{n-1}y\ \cdots\ x^{n-1}y^{m-1}\right)$$

avec n *et* m *les degrés de polynômes unitaires de* $\mathbb{Q}[X]$ *qui annulent* x *et* y *respectivement, puis montrer qu'il existe deux matrices* $A, B \in \mathcal{M}_{nm}(\mathbb{Q})$ *telles que* $AV^\top = xV^\top$ *et* $BV^\top = yV^\top$.

VI.35 Théorème de Kronecker ★★★★

[Corrigé]

Soit $P = \prod_{i=1}^{d}(X - \lambda_i) \in \mathbb{Z}[X]$ unitaire dont toutes les racines sont non nulle et de module inférieur à 1. Soit $k \in \mathbb{N}^*$.

1. Montrer que $\lambda_1^k, \dots, \lambda_d^k$ sont les racines d'un polynôme non nul Q_k unitaire à coefficients entiers.
   Indication : on pourra voir Q_k *comme un certain polynôme caractéristique*
2. Montrer que les coefficients de Q_k sont bornées.
3. En déduire que $\lambda_1, \dots, \lambda_d$ sont des racines de l'unité.

VI.36 Irrationalité de e (1) ★★

[Corrigé]

En utilisant $e = \sum_{k=0}^{+\infty} \frac{1}{k!}$ montrer que e est irrationnel.

VI.37 Irrationalité de e (2) ★★

[Corrigé]

On pose pour $n \in \mathbb{N}$, $I_n = \int_0^1 x^n e^x dx$.

1. Déterminer la limite de $(I_n)_{n\in\mathbb{N}}$.
2. En déduire que e est irrationnel.

VI.38 Irrationalité de π ★★★★

[Corrigé]

On pose pour $n \in \mathbb{N}$, $I_n = \int_0^\pi x^n (x-\pi)^n \sin(x) dx$.

1. Soit $n \in \mathbb{N}$. Montrer que I_n est un polynôme en π.
2. En déduire que π est irrationnel.

VI.39 Critère de transcendance de Liouville ★★★★

[Corrigé]

On dit qu'un nombre complexe est *transcendant* s'il n'est pas algébrique, autrement dit s'il n'est racine d'aucun polynôme non nul à coefficients rationnels.

1. Soit $\alpha \in \mathbb{C}$ un nombre algébrique. On se donne $(p_n) \in \mathbb{Z}^{\mathbb{N}}$ et $(q_n) \in (\mathbb{N}^*)^{\mathbb{N}}$ tels que la suite de rationnels $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}}$ converge vers α par valeurs différentes de α.

   Montrer qu'il existe un entier naturel non nul d tel que $\frac{1}{q_n^d} \underset{n\to+\infty}{=} \mathcal{O}\left(\alpha - \frac{p_n}{q_n}\right)$.

2. En déduire que la constante de Liouville $\sum_{n=1}^{+\infty} \frac{1}{10^{n!}}$ est un nombre transcendant.

VII

Arithmétique

VII.1 Infinité des nombres premiers ★★

[Corrigé]

1. Montrer qu'il existe une infinité de nombres premiers.
2. Montrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.

VII.2 Version faible du théorème de progression arithmétique de Dirichlet ★★★

[Corrigé]
Pour $n \in \mathbb{N}^*$ on note $\Phi_n = \prod_{\substack{1 \leq k \leq n \\ \text{pgcd}(k,n)=1}} \left(X - e^{\frac{2ik\pi}{n}}\right)$ le n-ième polynôme cyclotomique.

1. Montrer que $X^n - 1 = \prod_{d|n} \Phi_d$.
2. Montrer que $\forall n \in \mathbb{N}^*, \Phi_n \in \mathbb{Z}[X]$.
3. Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Que peut-on dire d'un nombre premier p qui divise $\Phi_n(a)$, mais aucun des $\Phi_d(a)$ pour d un diviseur strict positif de n ?
4. En déduire que pour $n \in \mathbb{N}^*$ fixé, il existe une infinité de nombre premier congrus à 1 modulo n.

VII.3 Racine carré d'un nombre premier ★★

[Corrigé]
Soit p un nombre premier. Démontrer que $\sqrt{p}$ est irrationnel.

VII.4 Une suite périodique ★★★

[Corrigé]
Soit $(P,Q) \in \mathbb{Z}[X]^2$ tel que $P \wedge Q = 1$. On pose pour $n \in \mathbb{N}$, $u_n = P(n) \wedge Q(n)$. Montrer que $(u_n)_{n\in\mathbb{N}}$ est périodique.

VII.5 Racines de l'unité ★★

[Corrigé]
Soit $(m,n) \in \mathbb{N}^*$. Montrer que $\mathbb{U}_n \cap \mathbb{U}_m = \mathbb{U}_{m\wedge n}$.

VII.6 Plus petit nombre premier ne divisant pas un entier donné

[Corrigé]

1. Montrer que tout entier $n > 6$ s'écrit comme la somme de deux entiers premiers entre eux, strictement supérieurs à 1.
2. Soit $(p_n)_{n\geq 1}$ la suite strictement croissante des nombres premiers. Montrer que pour tout $k > 2$, on a $p_{k+1} + p_{k+2} \leq p_1 p_2 \dots p_k$.
3. Pour $n \in \mathbb{N}^*$, on note q_n le plus petit nombre premier qui ne divise pas n. Montrer que la suite de terme général $\dfrac{q_n}{n}$ tend vers 0.

VII.7 Théorème de Kurshak ★★★★

[Corrigé]
Pour quelles valeurs entières de $n \geq m$ a-t-on $\displaystyle\sum_{i=m}^{n} \frac{1}{i} \in \mathbb{N}$?

VII.8 Valuation p-adique de $\binom{p^n}{k}$ ★★★

[Corrigé]
Soient p un nombre premier, $n \in \mathbb{N}^*$ et $k \in [\![1; p^n - 1]\!]$. Calculer la valuation p-adique de $\binom{p^n}{k}$.

VII.9 Une équation dans $\mathbb{N}$ ★★★

[Corrigé]
Résoudre dans $\mathbb{N}$, $a^b = b^a$

— Par une étude de fonction ;

— Par un raisonnement arithmétique.

VII.10 Triplets pythagoriciens ★★

[Corrigé]
Le but de cet exercice est de déterminer tous les triplets $(a, b, c) \in (\mathbb{N}^*)^3$ qui vérifient

$$a^2 + b^2 = c^2$$

1. Montrer qu'on peut se ramener à a, b, c premiers entre eux dans leur ensemble.
2. Montrer qu'on peut se ramener à a, b, c premiers entre eux deux à deux.
3. Montrer que parmi a, b et c il y en a deux qui sont pairs et un qui est impair.
4. Montrer que c est impair. On suppose désormais que c'est b qui est pair.
5. Montrer alors que, dans ce cas, (a, b, c) est un triplet pythagoricien si et seulement s'il existe deux entiers de parité différente et premier entre eux, u et v avec $u > v$ tels que :
$$a = u^2 - v^2 \quad , \quad b = 2uv, \quad c = u^2 + v^2$$
6. En déduire l'ensemble des triplets pythagoriciens.

VII.11 Théorème de Sophie Germain ★★★

[Corrigé]
Soit p un nombre premier de Sophie Germain, c'est à dire un nombre premier impair tel que $q = 2p + 1$ soit premier. On souhaite prouver que qu'il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0[p]$ et $x^p + y^p + z^p = 0$. Pour cela on raisonne par l'absurde et on se donne une telle solution (x, y, z).

1. Montrer que l'on peut se ramener à x, y, z premiers entre eux deux à deux.
2. a. Soit $k \in \mathbb{N}$. Montrer si le produit de deux entiers premiers entre eux est une puissance k-ième alors chacun des facteurs est une puissance k-ième.

   b. Montrer qu'il existe deux entiers a et α tels que $y+z = a^p$ et $\displaystyle\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = \alpha^p$. Etablir alors l'existence de deux entiers b et c tels que $x+y = c^p$ et $x+z = b^p$.
3. Montrer que si $m \in \mathbb{Z}$ n'est pas divisible par q alors $m^p \equiv \pm 1[q]$. En déduire qu'un et un seul des entiers x, y, z est divisible par q. On supposera dans la suite que c'est x.
4. Etablir successivement les congruences suivantes, toutes modulo q :

$$b^p + c^p - a^p \equiv 0 \ ; \ y \equiv c^p \ ; \ a \equiv 0 \ ; \ \alpha^p \equiv py^{p-1}$$

   Aboutir à une contradiction et conclure.

Il y a beaucoup de choses intéressantes à dire à propos de ce résultat. Sophie Germain (1776-1831) est quasiment la seule femme mathématicienne de son temps. Elle suivit les cours de l'École polytechnique par correspondance, car les femmes n'y étaient pas admises et c'est sous le pseudonyme masculin de Maurice Leblanc qu'elle écrivait à Gauss pour lui faire part de ses découvertes arithmétiques. Le théorème de Sophie Germain, démontré en 1823, est une résolution partielle du grand théorème de Fermat : Pour $n \geq 3$ et $(x, y, z) \in (\mathbb{N}^*)^3$ l'équation $x^n + y^n = z^n$ n'admet pas de solution.

VII.12 Une équation diophantienne ★★★

[Corrigé]
Soient $n \in \mathbb{N}$ et $\alpha \in \mathbb{N}$ tels que $\alpha > n \geq 2$. On cherche à montrer que l'équation

$$x_1^2 + \cdots + x_n^2 = \alpha x_1 \dots x_n$$

n'admet pas de solution entière non triviale (autre que $(0, \dots, 0)$).
Pour cela on raisonne par l'absurde : On se donne une solution $(x_1, \dots, x_n)$ non triviale pour laquelle on suppose sans perte de généralité que $x_1 \leq \cdots \leq x_n$.

1. Montrer que l'on peut trouver une autre solution de l'équation sous la forme $(x_1, \dots, x_{n-1}, y)$ avec $y < x_n$.
2. Conclure.

VII.13 Calcul d'une somme ★★★

[Corrigé]
Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$

1. Montrer que le quotient de la division euclidienne de a par b est $\left\lfloor \frac{a}{b} \right\rfloor$.
   On suppose dans la suite que $a \wedge b = 1$.

2. Montrer que l'application $\varphi : \left\{ \begin{array}{ccc} \mathbb{Z}/b\mathbb{Z} & \longrightarrow & \mathbb{Z}/b\mathbb{Z} \\ \overline{k} & \longmapsto & \overline{ak} \end{array} \right.$ est bijective.

3. Montrer que $\displaystyle\sum_{k=1}^{b-1} \left\lfloor \frac{ka}{b} \right\rfloor = \frac{(a-1)(b-1)}{2}$.

VII.14 Nombres de Mersenne ★★

[Corrigé]
Pour $n \in \mathbb{N}^*$ on appelle $n^{ème}$ nombre de Mersenne l'entier $M_n = 2^n - 1$.

1. a. Soient $n \in N^*$ et a un diviseur positif de n. Montrer que $2^a - 1$ divise M_n.
   b. En déduire que si M_n est un nombre premier, alors n est un nombre premier.
2. Soient p et q des nombres premiers avec p impair. On suppose que q divise M_p.
   a. Montrer que q est impair. En déduire que $2^{q-1} \equiv 1[q]$.
   b. En considérant l'ordre de $\overline{2}$ dans $(\mathbb{Z}/q\mathbb{Z})^*$, montrer que $q \equiv 1[p]$ puis que $q \equiv 1[2p]$.
3. Soient p un nombre premier impair et $n \in \mathbb{N}^*$ divisant M_p. En utilisant la décomposition en facteurs premiers de n, montrer que $n \equiv 1[2p]$.
4. Proposer un algorithme Python utilisant les résultats de l'exercice permettant de déterminer si le $n^{ème}$ nombre de Mersenne est premier.

Remarque : cet exercice montre que les nombres de Mersenne sont de bons candidats pour la recherche de grands nombres premiers... et pas qu'un peu ! Le plus grand nombre premier connu à ce jour est un nombre de Mersenne. Il a été découvert le 21 Octobre 2024 grâce au projet the Great Internet Mersenne Prime Search (GIMPS) qui rassemble les ordinateurs du monde pour la recherche de nombres de Mersenne premiers. Il s'agit de $2^{136279841} - 1$ *qui comporte pas moins de 41 024 320 chiffres !*

VII.15 Un exercice pour les années impaires ★★★★

[Corrigé]
Existe-t-il une application $f : \mathbb{N} \longmapsto \mathbb{N}$ telle que $\forall n \in \mathbb{N},\ f(f(n)) = n + 2025$?

VII.16 Equation du second degré dans $\mathbb{Z}/n\mathbb{Z}$ ★★

[Corrigé]
Résoudre dans $\mathbb{Z}/85\mathbb{Z}$ l'équation $x^2 - 3x + \overline{7} = \overline{0}$.

VII.17 Un problème de congruence ★★★

[Corrigé]
Montrer que $\forall n \in \mathbb{N}^*,\ 10^{10^n} \equiv 4[7]$.

VII.18 Un multiple de 2026 qui ne s'écrit qu'avec des 2 ★★★

[Corrigé]
Montrer qu'il existe un multiple de 2026 dont l'écriture décimale ne comporte que des 2.

VII.19 Somme des puissances k-ièmes dans $\mathbb{Z}/p\mathbb{Z}$ ★★★

[Corrigé]
Soient p un nombre premier et $k \in \mathbb{N}^*$. Calculer $S_k = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^k$

On pourra pour cela étudier les cas :

(i) k est multiple de $p-1$,

(ii) $d = \text{pgcd}(k, p-1) < p-1$ en calculant $y^k S_k$ pour $y \in (\mathbb{Z}/p\mathbb{Z})^*$.

On admettra qu'un polynôme à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ a toujours moins de racines que son degré.

VII.20 Théorème de Wilson ★★

[Corrigé]
Soit p un entier supérieur à 2. Montrer l'équivalence :

$$(p-1)! \equiv -1[p] \iff p \text{ est premier.}$$

VII.21 Problème Putnam (2011) ★★★★★

[Corrigé]
Soit p un nombre premier impair.
Montrer qu'il existe au moins $\dfrac{p+1}{2}$ valeurs de n dans $[\![0; p-1]\!]$ telles que p ne divise pas $\sum_{k=0}^{p-1} k! n^k$.

On admettra qu'un polynôme à coefficient dans $\mathbb{Z}/p\mathbb{Z}$ a toujours moins de racines que son degré.
ylo

VII.22 Critère d'Euler ★★★★

[Corrigé]
Soit p un nombre premier distinct de 2. On pose $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et $\mathbb{F}_p^* = \mathbb{F}_p \backslash \{\overline{0}\}$.

1. On pose $\mathcal{C} = \{x^2, x \in \mathbb{F}_p^*\}$. Montrer que $\text{Card}(\mathcal{C}) = \dfrac{p-1}{2}$.
2. Montrer que $a^{\frac{p-1}{2}} \in \{-\overline{1}, \overline{1}\}$.
3. Soient $d \in \mathbb{N}^*$ et $P \in \mathbb{Z}_{d-1}[X]$. Soit $(a_1, \dots, a_d) \in \mathbb{Z}^d$ telle que les a_i soient distincts modulo p et telle que $\forall i \in [\![1; d]\!],\ p | P(a_i)$. Montrer que $\forall n \in \mathbb{Z},\ p | P(n)$.
4. Montrer alors que $a^{\frac{p-1}{2}} = \begin{cases} \overline{1} & \text{si } a \in \mathcal{C} \\ -\overline{1} & \text{sinon} \end{cases}$

VII.23 Indicatrice d'Euler ★★★

[Corrigé]
Soit $n \in \mathbb{N}^*$. On note φ la fonction indicatrice d'Euler.

1. Soit d un diviseur positif de n. Montrer qu'il y a $\varphi(d)$ éléments d'ordre d dans le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.
2. Montrer que $n = \displaystyle\sum_{d|n} \varphi(d)$ où la somme porte sur les diviseurs positifs de n.
3. En déduire un programme Python permettant de calculer $\varphi(n)$.

VII.24 Une minoration de l'indicatrice d'Euler ★★★

[Corrigé]

1. Soient $n_1, \dots, n_k$ des entiers distincts supérieurs ou égaux à 2. Montrer que
$$\prod_{i=1}^{k} \left(1 - \frac{1}{n_i}\right) \geq \frac{1}{k+1}$$
2. On note φ la fonction indicatrice d'Euler. Montrer que
$$\forall n \in \mathbb{N}^*,\ \varphi(n) \geq \frac{n \ln 2}{\ln n + \ln 2}$$

VII.25 Théorème d'interversion de Möbius ★★★

[Corrigé]
Une fonction arithmétique est une fonction de $\mathbb{N}^*$ dans $\mathbb{C}$. On note 1, δ, I les fonctions arithmétiques :

$$1 : \begin{cases} \mathbb{N}^* & \longrightarrow & \mathbb{C} \\ n & \longmapsto & 1 \end{cases} \qquad \delta : \begin{cases} \mathbb{N}^* & \longrightarrow & \mathbb{C} \\ & & \\ n & \longmapsto & \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{sinon} \end{cases} \end{cases} \qquad I : \begin{cases} \mathbb{N}^* & \longrightarrow & \mathbb{C} \\ n & \longmapsto & n \end{cases}$$

On note μ la fonction de Möbius définie sur $\mathbb{N}^*$ par :

$$\mu(n) = \begin{cases} 0 & \text{si } n \text{ est divisible par le carré d'un nombre premier} \\ (-1)^k & \text{si } n \text{ est le produit de } k \text{ nombre premiers distincts} \end{cases}$$

On dit qu'une fonction arithmétique f est multiplicative quand :

$$\begin{cases} f(1) \neq 0 \\ \forall (m,n) \in (\mathbb{N}^*)^2,\ m \wedge n = 1 \Longrightarrow f(mn) = f(m)f(n) \end{cases}$$

Si f et g sont deux fonctions arithmétiques, le produit de convolution de f et g est la fonction la fonction arithmétique notée $f * g$ définie par :

$$\forall n \in \mathbb{N}^*,\ (f*g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

1. Montrer que μ est multiplicative.
2. Montrer que $\mu * 1 = \delta$.
3. Soit f et F deux fonctions arithmétiques telles que pour tout $n \in \mathbb{N}^*$, $F(n) = \sum_{d|n} f(d)$.

   Montrer que pour tout $n \in \mathbb{N}^*$,

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$$

4. Démontrer que $\varphi = \mu * I$ où φ désigne la fonction indicatrice d'Euler.

VII.26 Probabilité que deux entiers soient premiers entre eux ★★★★

[Corrigé]
Pour tout $n \in \mathbb{N}^*$, on note d_n le nombre de couple $(a,b) \in [\![1;n]\!]^2$ tel que a et b soient premiers entre eux. Soit μ la fonction de Möbius (définie dans l'exercice précédent).

1. Montrer que $d_n = \sum_{d=1}^{n} \mu(d) \left\lfloor \frac{n}{d} \right\rfloor^2$. On pourra utiliser la formule du crible (cf. VIII.13)
2. En déduire que $\frac{d_n}{n^2} \underset{n\to+\infty}{\longrightarrow} \frac{6}{\pi^2}$.

VII.27 Limite d'une fonction arithmétique multiplicative ★★★

[Corrigé]

Une fonction $f : \mathbb{N}^* \to \mathbb{C}$ est dite *multiplicative* lorsque $\forall n, m \in \mathbb{N}^*,\ n \wedge m = 1 \implies f(mn) = f(m)f(n)$.
On note $Q = \{p^k,\ p \text{ premier et } k \in \mathbb{N}^*\}$.

1. On se donne une fonction $f : \mathbb{N}^* \to \mathbb{C}$ multiplicative vérifiant :
$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N}^*,\ \forall q \in Q,\ q \geq N \implies |f(q)| \leq \varepsilon$$
Montrer que $\lim_{n\to+\infty} f(n) = 0$.
Indication : on pourra commencer par montrer que f est bornée.
2. On note φ la fonction indicatrice d'Euler. Montrer que φ est multiplicative et en déduire que :
$$\forall \delta \in]0, 1[,\ \lim_{n\to+\infty} \frac{n^{1-\delta}}{\varphi(n)} = 0$$
3. Que peut-on dire pour $\delta = 0$?

VII.28 Fonctions arithmétiques réelles additives ★★★★

[Corrigé]

On considère une fonction $f : \mathbb{N}^* \to \mathbb{R}$ croissante. On suppose que
$$\forall (m, n) \in (\mathbb{N}^*)^2,\ m \wedge n = 1 \implies f(mn) = f(m) + f(n)$$
On souhaite montrer qu'il existe $c \geq 0$ tel que $\forall n \in \mathbb{N}^*,\ f(n) = c\ln(n)$. On pose pour $n \in \mathbb{N}^*$ et $k \in \mathbb{N}$, $A_k(n) = \sum_{i=0}^{k} n^i$ et si $k \geq 1$, $B_k(n) = n^k - A_{k-1}(n)$. On pose aussi $B_0(n) = 1$. On fixe $n \geq 3$ un entier et $k \in \mathbb{N}^*$.

1. Montrer que $n \wedge A_k(n) = n \wedge B_k(n) = 1$.
2. Montrer que $f(A_k(n)) \geq kf(n)$ puis que $f(n^{k+1}) \geq kf(n)$.
3. Montrer que $f(B_k(n)) \leq kf(n)$ puis que $f(n^{k-1}) \leq kf(n)$.
4. En déduire que $f(n^k) = kf(n)$. Etendre l'égalité aux cas $n = 1$ et $n = 2$.
5. Conclure.

VII.29 Une majoration de la somme des diviseurs d'un entier ★★

[Corrigé]
On note pour $n \in \mathbb{N}^*$, $\sigma(n)$ la somme des diviseurs positifs de n. Montrer que $\sigma(n) \leq n + n\ln n$.

VII.30 Entiers algébriques ★★

[Corrigé]
On note $\tilde{\mathbb{Z}}[X]$ l'ensemble des polynômes **unitaires** à coefficients entiers et $\tilde{\mathbb{A}} = \{x \in \mathbb{C},\ \exists P \in \tilde{\mathbb{Z}}[X], P(x) = 0\}$ l'ensemble des entiers algébriques.
Montrer que $\tilde{\mathbb{A}} \cap \mathbb{Q} = \mathbb{Z}$.

VII.31 Majoration de la primorielle ★★★

[Corrigé]
On veut montrer que pour tout $n \in \mathbb{N}^*$, $\prod_{\substack{p \leq n \\ p \text{ premier}}} p \leq 4^n$.

1. Traiter les cas $n \in \{1, 2, 3\}$.

On suppose à présent $n \geq 4$ et le résultat connu au rang k pour tout entier k compris entre 1 et $n-1$.

2. Etablir le résultat au rang n quand n est pair.
3. Soit $n = 2m+1$ avec $m \in \mathbb{N}$. Justifier que $\prod_{\substack{m+1 \leq p \leq 2m+1 \\ p \text{ premier}}} p$ divise $\binom{2m+1}{m}$ et montrer que $\binom{2m+1}{m} \leq 4^m$.
4. Conclure.

VII.32 Théorèmes de Mertens ★★★

[Corrigé]
Soit $n \in \mathbb{N}^*$. Une somme indicée sur p indique que la sommation est effectuée sur les nombres premiers.
On admettra le résultat de l'exercice VII.31 et celui de la formule de Legendre VIII.11.

1. *Premier théorème de Mertens*

a. Montrer que :
$$\frac{n}{p} - 1 < \nu_p(n!) \leq \frac{n}{p}\frac{n}{p(p-1)}$$

b. Etablir que :
$$\sum_{k=1}^{n} \ln k = n\ln n - n + \mathcal{O}(\ln n)$$

c. Justifier que $n! = \prod_{p\leq n} p^{\nu_p(n!)}$ et en déduire que :
$$n\sum_{p\leq n}\frac{\ln p}{p} - n\ln 4 < \ln(n!) \leq n\sum_{p\leq n}\frac{\ln p}{p} + n\sum_{p\leq n}\frac{\ln p}{p(p-1)}$$

d. Justifier que la série $\sum_{k\geq 2}\frac{\ln k}{k(k-1)}$ converge.

e. Déduire de ce qui précède que $\sum_{p\leq n}\frac{\ln p}{p} \underset{n\to+\infty}{=} \ln n + \mathcal{O}(1)$

2. *Deuxième théorème de Mertens*

a. Soit $(a_n)_{n\geq 2}$ une suite de nombres réels. Pour $t \geq 2$, on pose $A(t) = \sum_{2\leq k\leq t} a_k := \sum_{k=2}^{\lfloor t\rfloor} a_k$. Soit $b : [2, +\infty[\to \mathbb{R}$ une fonction de classe $\mathcal{C}^1$.
Montrer que pour tout entier $n \geq 2$,
$$\sum_{k=2}^{n} a_k b(k) = A(n)b(n) - \int_2^n b'(t)A(t)dt$$

b. On pose pour tout $t \geq 2$,
$$R(t) = \sum_{p\leq t}\frac{\ln p}{p} - \ln t$$
Montrer que $\sum_{p\leq n}\frac{1}{p} = 1 + \ln(\ln n) - \ln(\ln 2) + \frac{R(n)}{\ln n} + \int_2^n \frac{R(t)}{t(\ln t)^2}dt$

c. Etablir que $\sum_{p\leq n}\frac{1}{p} \underset{n\to+\infty}{=} \ln(\ln n) + c + \mathcal{O}\left(\frac{1}{\ln n}\right)$ pour un réel $c \in \mathbb{R}$ à préciser.

VII.33 Théorèmes de Tchebychev ★★★

[Corrigé]
Soit $n \in \mathbb{N}^*$. Une somme indicée sur p indique que la sommation se fait sur les nombres

premiers.
On note pour $x \geq 1,\ \pi(x) = \sum_{p \leq x} 1 := \sum_{\substack{1 \leq p \leq \lfloor x \rfloor \\ p \text{ premier}}} 1 = \text{Card}(\{p \in [\![1; x]\!],\ p \text{ est premier}\})$.
On admettra le résultat des exercices VII.31 et celui de la formule de Legendre VIII.11.

1. *Minoration de Tchebytchev*
   a. Montrer que $\nu_p\left(\binom{2n}{n}\right) \leq \left\lfloor \frac{\ln(2n)}{\ln p} \right\rfloor$.
   b. Montrer que $\pi(2n) \geq \frac{\ln\left(\binom{2n}{n}\right)}{\ln(2n)}$.
   c. En déduire que APCR $\pi(2n) \geq c\frac{n}{\ln n}$ pour une constante c à préciser.
   d. Conclure en déterminant une minoration asymptotique de $\pi(n)$.
2. *Introduction d'une fonction auxiliaire*
   On note pour $x \geq 1\ \theta(x) = \sum_{p \leq x} \ln p$.
   a. Montrer que $\theta(x) \leq \pi(x) \ln x$.
   On fixe $\varepsilon > 0$.
   b. i. Montrer que $\theta(x) \geq (1-\varepsilon)\left(\pi(x) - \pi(x^{1-\varepsilon})\right) \ln x$.
   ii. Montrer que $\pi(x^{1-\varepsilon}) \underset{x \to +\infty}{=} o(\pi(x))$.
   iii. En déduire que $\forall \eta > 0,\ \exists x_0 \geq 1,\ \forall x \geq x_0,\ \theta(x) \geq (1-\varepsilon)\pi(x)\ln x + \eta\pi(x)\ln x$.
   c. Démontrer que $\theta(x) \underset{x \to +\infty}{\sim} \pi(x) \ln x$.
3. *Majoration de Tchebytchev*
   a. Montrer que $\theta(2n) - \theta(n) \leq n \ln 4$.
   b. Montrer que pour tout $x \geq 1,\ \theta(2x) - \theta(2\lfloor x \rfloor) \leq 2\ln(2x)$ et $\theta(x) - \theta(\lfloor x \rfloor) \leq \ln x$.
   c. En déduire qu'il existe une constante $C > 0$ telle que $\forall x \geq 1,\ \theta(2x) - \theta(x) \leq x \ln 4 + C \ln x$.
   d. Montrer que $\forall n \in \mathbb{N},\ \theta(x) \leq \theta\left(\frac{x}{2^n}\right) + x \ln 2 \sum_{k=0}^{n-1} \frac{1}{2^k} + nC \ln x$.
   e. Conclure en déterminant une majoration asymptotique de $\theta(x)$ puis de $\pi(x)$.

VIII

Dénombrement

VIII.1 Identité de Vandermonde ★★

[Corrigé]
Soient r, m, n des entiers naturels. Montrer que :

$$\sum_{k=0}^{r} \binom{n}{k}\binom{m}{r-k} = \binom{n+m}{r}$$

VIII.1.1 Formule de Chu-Vandermonde

Pour $\alpha \in \mathbb{R}$, on pose

$$\forall n \in \mathbb{N}, \binom{\alpha}{n} = \frac{\alpha(\alpha-1)\dots(\alpha-n+1)}{n!}$$

Etablir que :

$$\forall (a,b) \in \mathbb{R}, \sum_{k=0}^{n} \binom{a}{k}\binom{b}{n-k} = \binom{a+b}{n}$$

VIII.2 Nombre de Fibonacci ★★★

[Corrigé]
Déterminer le nombre a_n de manière de recouvrir un damier de dimension $2 \times n$ avec des pièces de dimension 1×2. Montrer que si n est assez grand a_n est la partie entière de $\frac{1}{2} + \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1}$.

VIII.3 Matrices orthogonales à coefficients entiers ★★

[Corrigé]
Quel est le cardinal de $\mathcal{O}_n(\mathbb{R}) \cap \mathcal{M}_n(\mathbb{Z})$?

VIII.4 Nombre de carrés inférieur à un entier fixé ★

[Corrigé]
Pour tout $n \in \mathbb{N}$, on pose $A(n)$ l'ensemble des carrées d'entiers non nuls inférieur à n.
Déterminer le cardinal de $A(n)$.

VIII.5 Dérangement ★★★

[Corrigé]

1. Calculer $\displaystyle\sum_{k=0}^{p}(-1)^k\binom{n}{k}\binom{n-k}{p-k}$ pour $0 \leq p \leq n$.
2. Soit D_n le nombre de permutations de $\mathfrak{S}_n$ n'ayant pas de point fixe. Montrer que $\displaystyle\sum_{k=0}^{n}\binom{n}{k}D_k = n!$
   (on pose $D_0 = 1$)
3. Etablir, par une preuve combinatoire, que pour tout $n \geq 2$, $D_{n+1} = n(D_n + D_{n-1})$
4. En déduire que pour tout $n \geq 2$, $D_n = nD_{n-1} + (-1)^n$.
5. Retrouver la valeur de D_n.
6. Montrer que $D_n = n!\displaystyle\sum_{k=0}^{n}\frac{(-1)^k}{k!}$
7. On considère la série entière $\displaystyle\sum_{n=0}^{+\infty}\frac{D_n}{n!}z^n$, (série génératrice exponentielle de la suite $(D_n)_{n\in\mathbb{N}}$).
   On note D sa somme.
   Minorer son rayon de convergence R et calculer $D(z)$ pour $|z| < R$.
8. En déduire que D_n est la partie entière de $\dfrac{n!}{e} + \dfrac{1}{2}$.

Remarque : Ce dernier résultat correspond au problème des rencontres ou encore problème de Montmort.

VIII.6 Dérangement partiel ★★★

[Corrigé]
On pose $D_0 = 1$ et, pour $n \in \mathbb{N}^*$, on note D_n le nombre de permutation de $[\![1;n]\!]$ n'ayant pas de point fixe.

1. Quel est le nombre moyen de points fixes de $\sigma \in S_n$?

2. a. Montrer que $n! = \sum_{k=0}^{n} \binom{n}{k} D_k$

   b. En déduire que $D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$

   c. Montrer que le nombre de permutations de $[\![1;n]\!]$ admettant exactement p points fixes est : $\frac{n!}{p!} \sum_{k=0}^{n-p} \frac{(-1)^k}{k!}$.
   En déduire que :
   $$\sum_{p=1}^{n} \frac{1}{(p-1)!} \sum_{k=0}^{n-p} \frac{(-1)^k}{k!} = 1$$

VIII.7 Nombres de Bell ★★★

[Corrigé]
Pour tout $n \in \mathbb{N}^*$, on note B_n le nombre de partitions de l'ensemble $[\![1;n]\!]$. Par convention on pose $B_0 = 1$.

1. Calculer B_1, B_2 et B_3.

2. Montrer que $\forall n \in \mathbb{N},\ B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_{n-k}$.

3. On pose $f(z) = \sum_{n=0}^{+\infty} \frac{B_n}{n!} z^n$.
   Montrer que le rayon de convergence R de cette série entière n'est pas nul. Calculer $f(z)$ pour $z \in]-R, R[$.
   Exprimer B_n comme somme d'une série.

Remarque : Il en résulte des calculs précédents que le rayon de convergence de la série entière définissant f est en fait infini. Cette formule peut servir de point de départ à l'étude asymptotique de la suite (B_n). Le lecteur intéressé pourra par exemple étudier la première épreuve du concours Mines-Ponts de 2002 qui se propose d'obtenir un équivalent de B_n.

VIII.8 Nombres de Catalan ★★★

[Corrigé]
On s'intéresse à des chaînes de caractères constitués uniquement des deux caractères, parenthèse ouvrante et parenthèse fermante. On dit qu'un mot est *bien parenthésé* s'il commence par une parenthèse ouvrante et qu'à toute parenthèse ouvrante est associée une (unique) parenthèse fermante qui lui est postérieure.
Par exemple le mot ()(()) est bien parenthésé. En revanche, le mot ())() n'est pas bien parenthésé.
Un mot bien parenthésé est ainsi forcément constitué d'un nombre pair de caractères : chaque parenthèse qui s'ouvre doit se refermer. Pour tout entier $n \geq 1$, on note C_n le nombre de mots bien parenthésés de longueurs $2n$. On pose par commodité $C_0 = 1$.

1. Montrer que $\forall n \in \mathbb{N}$, $C_{n+1} = \sum_{k=0}^{n} C_k C_{n-k}$.
2. Montrer que, pour tout entier naturel n, $C_n \leq 2^{2n}$. Que peut-on dire du rayon de convergence de la série entière $\sum_{n\in\mathbb{N}} C_n x^n$.

Pour tout $x \in]-\frac{1}{4}, \frac{1}{4}[$, on pose $F(x) = \sum_{n=0}^{+\infty} C_n x^n$.

3. Montrer que, pour tout $x \in]-\frac{1}{4}, \frac{1}{4}[$, $F(x) = 1 + x(F(x))^2$
4. Montrer que la fonction $f : x \in]-\frac{1}{4}, \frac{1}{4}[\mapsto 2xF(x) - 1$ ne s'annule pas.
5. Déterminer, pour tout $x \in]-\frac{1}{4}, \frac{1}{4}[$, une expression de $F(x)$ en fonction de x.
6. Déterminer le développement en série entière de la fonction $u \mapsto \sqrt{1-u}$. On écrira les coefficients sous la forme d'un quotient de factorielles et de puissances de 2.
7. Montrer que, pour tout entier naturel n,

$$C_n = \frac{(2n)!}{(n+1)!n!}$$

VIII.9 Nombres de parties ★★

[Corrigé]
Soit E un ensemble possédant $n \in \mathbb{N}^*$ éléments. On désigne par $\mathcal{P}(E)$ l'ensemble des parties de E.

1. Déterminer le nombre de couples $(A, B) \in (\mathcal{P}(E))^2$ tels que $A \subset B$
2. Déterminer le nombre de couples $(A, B) \in (\mathcal{P}(E))^2$ tels que $A \cap B = \emptyset$
3. Déterminer le nombre de triplets $(A, B, C) \in (\mathcal{P}(E))^3$ tels que A, B et C soient deux à deux disjoints et vérifient $A \cup B \cup C = E$.

VIII.10 Nombre de surjection ★★★

[Corrigé]
Soient $(n,p) \in (\mathbb{N}^*)^2$, on note $S(n,p)$ le nombre de surjections d'un ensemble à n éléments vers un ensemble à p éléments.

1. Vérifier que $S(n,p) = n!$ si $n = p$ et $S(n,p) = 0$ si $n < p$.
   On pose par convention $S(0,0) = 1,\ S(0,p) = S(n,0) = 0$ si $(n,p) \in (\mathbb{N}^*)^2$.
2. Montrer que $p^n = \sum_{k=0}^{p} \binom{p}{k} S(n,k)$.
3. En déduire une expression de $S(n,p)$.

VIII.11 Formule de Legendre ★★★

[Corrigé]
Démontrer que pour tout p premier et $n \in \mathbb{N}$, $v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$

VIII.12 Théorème de Hall ★★★★

[Corrigé]
Soient $n \in \mathbb{N}^*$ et E un ensemble fini. Considérons $A_1, \dots, A_n \subset E$. Montrer que les assertions suivantes sont équivalentes :

(i) $\exists (x_1, \dots, x_n) \in \prod_{k=1}^{n} A_k,\ \forall (i,j) \in [\![1;n]\!]^2, (i \neq j \implies x_i \neq x_j)$

(ii) $\forall I \subset [\![1;n]\!],\ \mathrm{Card}\left(\bigcup_{i \in I} A_i\right) \geq \mathrm{Card}(I)$

VIII.13 Formule du Crible ★★★

[Corrigé]
Soient E un ensemble fini et $(A_i)_{1 \leq i \leq n}$ une famille de parties de E. Montrer que :

$$\mathrm{Card}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{k=1}^{n} \left((-1)^{k+1} \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} \mathrm{Card}\left(\bigcap_{j=1}^{k} A_{i_j}\right)\right)$$

VIII.14 Cardinal de $\mathrm{GL}_n(K)$ et $\mathrm{SL}_n(K)$ ★★★★ (HP)

[Corrigé]
Soit K un corps commutatif fini de cardinal q.

1. Déterminer le cardinal de $\mathrm{GL}_n(K)$.
2. En déduire le cardinal de $\mathrm{SL}_n(K)$.

VIII.15 $\mathbb{Q}$ est dénombrable ★★

[Corrigé]

1. Montrer que $\mathbb{Z}$ est dénombrable.
2. Montrer que $\mathbb{N}^2$ est dénombrable.
3. En déduire que le produit cartésiens d'un nombre fini d'ensembles au plus dénombrables est au plus dénombrable.
4. Montrer que $\mathbb{Q}$ est dénombrable.

VIII.16 $\mathbb{R}$ n'est pas dénombrable ★★★

[Corrigé]
Soit $f : \mathbb{N}^* \to [0, 1[$. Pour chaque $k \in \mathbb{N}^*$, on note u_k la k-ième décimale du développement décimal propre de $f(k)$ et on pose $v_k = 0$ si $u_k = 1$ et $v_k = 1$ sinon. Montrer que $y = 0, v_1 v_2 \dots v_n \dots$ n'a pas d'antécédent par f. Que dire ?

VIII.17 Dénombrabilité des nombres algébriques ★★★

[Corrigé]
Montrer que l'ensemble des nombres complexes qui sont racine d'un polynôme non nul à coefficients rationnels est dénombrable.

VIII.18 Théorème de Cantor ★★★

[Corrigé]
Soit E un ensemble. Montrer qu'il n'existe pas de surjection de $\mathcal{P}(E)$ dans E.
En déduire que l'ensemble des parties d'un ensemble dénombrable n'est pas dénombrable.

VIII.19 Fonction qui intervertit rationnels et irrationnels ★★★

[Corrigé]
Existe-t-il une fonction continue $f : \mathbb{R} \to \mathbb{R}$ telle que $f(\mathbb{Q}) \subset \mathbb{R}\backslash\mathbb{Q}$ et $f(\mathbb{R}\backslash\mathbb{Q}) \subset \mathbb{Q}$.

VIII.20 Support d'une famille sommable ★★

[Corrigé]
Soit $(a_i)_{i\in I}$ une famille sommable de nombres complexes. Montrer que son support $S = \{i \in I,\ a_i \neq 0\}$ est au plus dénombrable.

VIII.21 Théorème de Froda ★★★

[Corrigé]
Soit f une fonction monotone sur un intervalle I de $\mathbb{R}$. On définit l'oscillation de f en $x \in I$ par $\omega(x) = \left|\lim_{x^+} f - \lim_{x^-} f\right|$.
Justifier que ω est bien définie sur I puis montrer que l'ensemble des points de discontinuité de f est au plus dénombrable.

VIII.22 Ensemble discret ★★

[Corrigé]
Soit E un espace vectoriel normé. On dit qu'un point x d'une partie A de E est isolé lorsqu'il existe un voisinage $\mathcal{V}(x)$ de x tel que $\mathcal{V}(x) \cap A = \{x\}$. Lorsque tous les points de A sont isolés, on dit que A est un ensemble discret.
Remarque : Un point qui n'est pas isolé est aussi appelé point d'accumulation.

1. L'ensemble $A = \left\{\frac{1}{n},\ n \in \mathbb{N}^*\right\}$ est-t-elle une partie discrète de $\mathbb{R}$? Même question pour $B = A \cup \{0\}$.
2. Montrer qu'une partie discrète de $\mathbb{R}$ est au plus dénombrable.
3. Une partie dénombrable de $\mathbb{R}$ est-elle forcément dénombrable ?

VIII.23 Ensemble parfait

[Corrigé]
Soit E un espace vectoriel normé. Un sous-ensemble A de E est dit *parfait* s'il est fermé et n'a aucun point isolé (cf. VIII.22.

VIII.23.1 Poussière de Cantor

On admet (cf. XII.7) que tout réel $x \in [0,1[$ s'écrit de manière unique $x = \sum_{n=1}^{+\infty} \frac{a_n}{3^n}$ où $(a_n)_{n\in\mathbb{N}^*}$ une suite à valeurs dans $\{0,1,2\}$ qui ne stationne pas à 2. On définit *l'ensemble de Cantor* $K = \left\{ \sum_{n=1}^{+\infty} \frac{a_n}{3^n} \mid \forall n \in \mathbb{N}^*,\ a_n \in \{0,2\} \right\}$.
Montrer que K est un ensemble parfait, d'intérieur vide, compact et non dénombrable.

VIII.23.2 Ensemble parfait de $\mathbb{R}$

1. Donner un exemple d'ensemble parfait de $\mathbb{R}$.
2. Montrer qu'un ensemble parfait non vide de $\mathbb{R}$ n'est pas dénombrable.
3. Montrer que l'intervalle $]0,1[$ n'est pas réunion dénombrable de segments disjoints.

VIII.23.3 Théorème de Cantor-Bendixson

Montrer que toute partie fermée de $\mathbb{R}$ se décompose de façon unique comme réunion disjointe d'une partie dénombrable et d'un ensemble parfait.

IX

Probabilités

Dans toute cette section les variables aléatoires sont définies sur un univers Ω au plus dénombrable.

IX.1 Somme de variables de Bernoulli indépendantes ★★

[Corrigé]
Soient $X_1, \dots, X_n$ des variables indépendantes et identiquement distribuées suivant une loi de Bernoulli de paramètre $p \in]0,1[$. Montrer que $X = X_1 + \cdots + X_n$ suit une loi binomiale de paramètres n et p.

IX.2 Approximation d'une loi de Poisson par des lois binomiales ★

[Corrigé]
Soit $(X_n)_{n\geq 1}$ une suite de variables aléatoires telle que, $\forall n \geq 1,\ X_n \sim \mathcal{B}(n, p_n)$. On suppose que la suite $(np_n)_{n\geq 1}$ converge vers un réel $\lambda > 0$.
Démontrer que pour tout $k \in \mathbb{N}$, $\lim\limits_{n\to+\infty} \mathbb{P}(X_n = k) = \dfrac{\lambda^k e^{-\lambda}}{k!}$

IX.3 Inégalité de Markov et inégalité de Bienaymé-Tchébychev ★

[Corrigé]
Enoncer et démontrer les inégalités de Markov et de Bienaymé-Tchébychev.

IX.3.1 Utilisation de l'inégalité de Bienaymé-Tchebychev

Soit X une variable aléatoire discrète telle que $\mathbb{E}(X) = 10$ et $\mathbb{V}(X) = 5$. Montrer que :

$$\forall n \in \mathbb{N},\ n \geq 50 \implies \mathbb{P}(10 - n < X < 10 + n) \geq 0.99$$

IX.4 Paradoxe des anniversaires ★★

[Corrigé]
On considère une classe de n élèves. Pour chaque élève, on suppose que chaque jour de l'année a la même probabilité d'être le jour de son anniversaire et on ne prend pas en compte les années bissextiles.
Calculer la probabilité p_n que deux élèves au moins de cette classe aient leur anniversaire le même jour. A partir de combien d'élèves cette probabilité devient-elle supérieure à $0,5$? Combien vaut-elle si $n = 50$?

IX.4.1 Généralisation ★★★

On cherche désormais la probabilité $p_{k,n}$ que k élèves d'une classe de n élèves aient la même date d'anniversaire.

1. Ecrire un programme python calculant $p_{k,n}$.
2. Déterminer une expression de $p_{k,n}$ à l'aide de la formule du crible (cf. VIII.13).

IX.5 Variable aléatoire presque sûrement nulle/constante ★★

[Corrigé]

1. Soit X une variable aléatoire discrète telle que $\mathbb{E}(|X|) = 0$.
   Montrer que X est presque sûrement nulle, c'est-à-dire que $\mathbb{P}(X = 0) = 1$.
2. Soit X une variable aléatoire discrète telle que $\mathbb{V}(X) = 0$.
   Montrer que X est presque sûrement constante, c'est à dire qu'il existe $a \in X(\Omega)$, $\mathbb{P}(X = a) = 1$.

IX.6 Loi de Pascal ★★

[Corrigé]
Soit $(X_n)_{n\geq 1}$ une suite de variables indépendantes et identiquement distribuées selon une loi de Bernoulli de paramètre $p \in]0,1[$.
Pour $r \in \mathbb{N}^*$, on définit une variable aléatoire T_r à valeurs dans $\mathbb{N}^* \cup \{+\infty\}$ en posant :

$$T_r = \min(\{n \in \mathbb{N}^* | X_1 + \cdots + X_n = r\})$$

1. Reconnaître la loi de T_r lorsque $r = 1$.
2. Soit $r > 1$. Pour $n \in \mathbb{N}^*$ déterminer $\mathbb{P}(X_1 + \cdots + X_n = r-1)$ et en déduire $\mathbb{P}(T_r = n)$.
3. Montrer que l'événement $\{T_r = +\infty\}$ est négligeable.

IX.7 Lemme de Borel-Cantelli et loi du zéro-un de Borel ★★★

[Corrigé]
Soit $(A_n)_{n\in\mathbb{N}}$ une suite d'événements d'un espace probabilisé $(\Omega, \mathcal{A}, \mathbb{P})$. On pose $B_n = \bigcup_{k\geq n} A_k$ et $A = \bigcap_{n\in\mathbb{N}} B_n$.

1. On suppose que la série $\sum_{n\in\mathbb{N}} \mathbb{P}(A_n)$ converge.
   a. Montrer que $\mathbb{P}(A) = \lim_{n\to+\infty} \mathbb{P}(B_n)$.
   b. En déduire que $\mathbb{P}(A) = 0$.
2. On suppose que les A_n sont mutuellement indépendants et que la série $\sum_{n\in\mathbb{N}} \mathbb{P}(A_n)$ diverge.
   a. Soit $(n,p) \in \mathbb{N}^2$. Montrer que
   $$\mathbb{P}\left(\bigcap_{k=n}^{n+p} \overline{A_k}\right) \leq \exp\left(-\sum_{k=n}^{n+p} \mathbb{P}(A_k)\right)$$
   b. En déduire que $\mathbb{P}(A) = 1$.

IX.8 Formule d'antirépartition ★★★

[Corrigé]
Soit X une variable aléatoire à valeurs dans $\mathbb{N}$. Montrer que X admet une espérance finie si et seulement si la série $\sum_{n\in\mathbb{N}} \mathbb{P}(X > n)$ converge et que, dans ce cas, $\mathbb{E}(X) = \sum_{n=0}^{+\infty} \mathbb{P}(X > n)$.

IX.9 Loi de Poisson ★★

[Corrigé]
On considère un péage composé de m guichets. On note N la variable aléatoire égale au nombre de voitures utilisant le péage en 1h. N suit une loi de Poisson de paramètre $\lambda > 0$. Le choix du guichet se fait de manière aléatoire et indépendamment des autres voitures. On note X la variable aléatoire égale au nombre de voitures ayant pris le guichet n°1.

1. Calculer la probabilité conditionnelle $\mathbb{P}(X = k|N = n)$ pour $0 \leq k \leq n$.
2. Montrer que $\mathbb{P}(X = k) = e^{-\lambda}\frac{1}{k!}\left(\frac{\lambda}{m}\right)^k \sum_{n=0}^{+\infty} \lambda^n \left(1 - \frac{1}{m}\right)^n \frac{1}{n!}$.
3. Donner la loi de X.
4. Espérance et variance de X ?

IX.10 Maximum de deux lois géométriques indépendantes ★

[Corrigé]
Soient X et Y deux variables aléatoires indépendantes suivant des lois géométriques de paramètres respectifs p et q non égaux à 0 ou 1.

1. Déterminer l'espérance de $M = \min(X, Y)$.
2. Déterminer l'espérance de $Z = \max(X, Y)$.

IX.11 Max et min de lois géométriques iid ★★★★

[Corrigé]
Soit $(X_n)_{n\geq 1}$ une suite de variables indépendantes et identiquement distribuées selon une loi géométrique de paramètre $p \in]0, 1[$. Pour $n \in \mathbb{N}^*$, on pose :

$$Y_n = \min\{X_1, \dots, X_n\} \text{ et } Z_n = \max\{X_1, \dots, X_n\}$$

1. Calculer $\mathbb{E}(Y_n)$.
2. Déterminer un équivalent de $\mathbb{E}(Z_n)$ lorsque n tend vers l'infini.

IX.12 Formule de Wald ★★★

[Corrigé]
Soit X une variable aléatoire à valeurs dans $\mathbb{N}$ sur un espace probabilisé $(\Omega, \mathcal{A}, \mathbb{P})$. On considère une suite $(X_n)_{n\in\mathbb{N}^*}$ de variables aléatoires indépendantes sur $(\Omega, \mathcal{A}, \mathbb{P})$ suivant la même loi que X.

On se donne une autre variable aléatoire N à valeurs dans $\mathbb{N}^*$ sur le même espace probabilisé $(\Omega, \mathcal{A}, \mathbb{P})$ indépendante des variables aléatoires précédentes.
On pose $S = \sum_{k=1}^{N} X_k$, c'est-à-dire :

$$\forall \omega \in \Omega,\ S(\omega) = \sum_{k=1}^{N(\omega)} X_k(\omega)$$

1. Justifier que S est bien une variable aléatoire discrète.
2. On note G_X, G_N et G_S les fonctions génératrices respectives de X, N et S Montrer que pour tout $t \in [0,1], G_S(t) = G_N \circ G_X(t)$.
3. On suppose que les variables aléatoires X et N admettent des espérances finies. Montrer qu'il en est de même pour S et exprimer son espérance en fonction de celles de N et X.
4. On suppose que les variables aléatoires X et N admettant des variances finies. Montrer qu'il en est de même pour S et exprimer sa variance en fonction des espérances et des variances de N et X.

IX.13 Loi binomiale aléatoire ★★★

[Corrigé]
Sur un espace probabilisé $(\Omega, \mathcal{A}, \mathbb{P})$, on considère une suite $(X_n)_{n\in\mathbb{N}}$ de variables aléatoires et $p \in]0,1[$ telles que
$\forall n \in \mathbb{N},\ X_n \sim \mathcal{B}(n,p)$.
On considère aussi une variable aléatoire N indépendante des variables X_n et telle que $N+1 \sim \mathcal{G}(q)$ avec $q \in]0,1[$.
Pour toute issue ω de l'univers Ω, on pose $Y(\omega) = X_{N(\omega)}(\omega)$.
Justifier que Y est bien une variable aléatoire discrète et déterminer sa loi.

IX.14 Somme de lois de Poisson ★

[Corrigé]
Soient $\lambda_1, \dots, \lambda_n$ des réels et $X_1, \dots, X_n$ des variables aléatoires indépendantes telles que $\forall i \in [\![1; n]\!],\ X_i \sim \mathcal{P}(\lambda_i)$.
Montrer que $S = \sum_{i=1}^{n} X_i$ suit une loi de Poisson dont on précisera le paramètre.

IX.15 Obtenir trois pile consécutifs ★★★

[Corrigé]

1. Montrer que $X^3 - X^2 - X - 1 = (X - a)(X - b)(X - \bar{b})$ avec $a \in]1; 2[$, $b \in \mathbb{C} \setminus \mathbb{R}$ et $|b| < 1$.
2. On lance une infinité de fois une pièce équilibrée. On note p_n la probabilité pour que la séquence PPP apparaisse pour la première fois au n-ième lancer. Exprimer p_{n+3} en fonction de p_n, p_{n+1} et p_{n+2}.
3. Donner une expression et un équivalent de p_n.

IX.16 Lancer de dés équitable ★★★

[Corrigé]
On lance deux dés à 6 faces numérotées de un à six et on note X la somme obtenue. Les deux lancées sont supposés indépendants.
En truquant convenablement les 2 dés, X peut-elle suivre la loi uniforme sur $[\![2; 12]\!]$?

IX.16.1 Généralisation ★★★★

On lance n dés à m faces numérotées de 1 à m. On note pour $k \in [\![1; n]\!]$, X_k la variable aléatoire qui donne le numéro obtenu pour le k-ième dé. On note $S = \sum_{k=1}^{n} X_k$.
En truquant convenablement les dés, S peut-elle suivre une loi uniforme sur $[\![n; nm]\!]$?

IX.17 Espérance conditionnelle ★★★

[Corrigé]
Soit X une variable aléatoire discrète sur un espace probabilisé $(\Omega, \mathcal{A}, \mathbb{P})$ à valeurs dans $\mathbb{K}$. Pour A un événement non négligeable et sous réserve d'existence, on introduit l'espérance conditionnelle de X sachant A comme étant égale à l'espérance de X pour la probabilité conditionnelle $\mathbb{P}_A$, c'est-à-dire :

$$\mathbb{E}_A(X) = \sum_{x \in X(\Omega)} x\mathbb{P}_A(X = x)$$

On suppose que X est d'espérance finie.

1. Justifier l'existence de $\mathbb{E}_A(X)$ et vérifier que $\mathbb{E}_A(X) = \dfrac{\mathbb{E}(\mathbb{1}_A \cdot X)}{\mathbb{P}(A)}$.
2. Soit $(A_i)_{i \in I}$ un système complet d'événements non négligeables. Vérifier que $\mathbb{E}(X) = \sum_{i \in I} \mathbb{E}_{A_i}(X)\mathbb{P}(A_i)$

IX.18 Problème du collectionneur ★★

[Corrigé]
Un étudiant en classe préparatoire achète des cartes ©Pokémon TCG Pocket pour compléter un set contenant n cartes, où n est un entier naturel supérieur ou égal à 2. Lorsqu'on achète une carte, celle-ci est cachée et on ne peut la choisir. On s'intéresse au nombre d'achats nécessaires pour le set. On suppose que la répartition des n cartes est uniforme au cours de tous les achats, si bien qu'on assimile l'expérience aléatoire "acheter une carte" à un tirage avec remise d'une carte (numéroté entre 1 et n) dans un booster contenant les n cartes.
On note T_n la variable aléatoire égale au nombre de tirages nécessaires pour obtenir pour la première fois au moins chacune des n cartes. A chaque tirage, on appelle succès le fait d'avoir tiré un carte non encore obtenue. Pour $i \in [\![1;n]\!]$, on note $X_{n,i}$ la variable aléatoire donnant le nombre de tirages nécessaires pour obtenir pour la première fois i numéros différents, en comptant à partir du succès précédent. Par convention, $X_{n,1} = 1$ et on a ainsi $T_n = \sum_{i=1}^{n} X_{n,i}$.

1. Soit $i \in [\![2;n]\!]$.Déterminer la loi de $X_{n,i}$ et donner, sous réserve d'existence, l'espérance et la variance de $X_{n,i}$.
2. Justifier que les variables aléatoires $(X_{n,i})_{i\in[\![1;n]\!]}$ sont mutuellement indépendantes.
3. En déduire une expression de $\mathbb{E}(T_n)$ et $\mathbb{V}(T_n)$ faisant intervenir $H_n = \sum_{k=1}^{n} \frac{1}{k}$ et $S_n = \sum_{k=1}^{n} \frac{1}{k^2}$.
4. Donner des équivalents simples de $\mathbb{E}(T_n)$ et $\mathbb{V}(T_n)$.

IX.18.1 Généralisation

Soient $X_1, \dots, X_n$ des variables aléatoires i.i.d. suivant la loi d'une variable aléatoire X fixée à valeur dans $\mathbb{N}$. On note $R_n = \text{Card}(\{X_1, \dots, X_n\})$.

1. Soit $a \in \mathbb{R}_+$. Montrer que $\mathbb{E}(R_n) \leq a + n\mathbb{P}(X \geq a)$.
2. En déduire que $\mathbb{E}(R_n) \underset{n\to+\infty}{=} o(n)$.
3. Montrer que si X admet une espérance finie, on a même $\mathbb{E}(R_n) \underset{n\to+\infty}{=} \mathcal{O}(\sqrt{n})$.
   Indication : Penser à l'inégalité de Markov

IX.19 Problème de la ruine du joueur

[Corrigé]
Deux personnes A et B jouent à pile ou face avec une pièce qui a une probabilité p de tomber sur pile et $1-p$ de tomber sur face. Le joueur A possède au début du jeux un capital de a euros et le joueur B un capital de b euros. A chaque lancer, si la pièce tombe sur pile le

joueur A donne un euro au joueur B, sinon c'est le joueur B qui donne un euro au joueur A. Ils continuent de jouer jusqu'à que l'un d'eux soit ruiné.

1. Quelle est la probabilité que le joueur A finisse ruiné ?
2. Et si le joueur A joue au même jeux contre le casino ?

IX.20 Passager d'un avion

[Corrigé]
100 passagers s'apprêtent à monter dans un avion de 100 places. Le premier passager entre et s'assied à une place au hasard. Les suivants prennent leur place si elle est disponible, et choisissent une place libre au hasard sinon. Quelle est la probabilité que le dernier passager se retrouve à sa place ?

IX.21 Fonction de répartition ★★★★

[Corrigé]
Soit X une variable aléatoire discrète à valeurs réelles.
On appelle *fonction de répartition* de la variable X, l'application $F_X : \mathbb{R} \to \mathbb{R}$ définie par :

$$F_X(x) = \mathbb{P}(X \leq x) \text{ pour tout } x \in \mathbb{R}.$$

1. Montrer que la fonction F_X est croissante et déterminer ses limites en $\pm\infty$.
2. Montrer que la fonction F_X est continue à droite en tout point.
3. A quelle condition F_X est-elle continue en un point a de $\mathbb{R}$?

IX.22 Loi sans mémoire ★★

[Corrigé]
Soit X une variable aléatoire à valeurs dans $\mathbb{N}^*$. Montrer que X suit une loi géométrique si et seulement si

$$\forall (n,k) \in \mathbb{N}^2,\ \mathbb{P}(X > n+k | X > n) = \mathbb{P}(X > k)$$

IX.23 Caractérisation de la loi de Poisson par l'espérance

[Corrigé]
Soit $(\Omega, A, \mathbb{P})$ un espace probabilisé.

1. Soient $\lambda > 0$ et N une variable aléatoire suivant la loi de Poisson $\mathcal{P}(\lambda)$.
   Montrer que si g est une fonction de $\mathbb{N}$ dans $\mathbb{N}$, alors $\mathbb{E}(Ng(N)) = \lambda \mathbb{E}(g(N+1))$.

2. Soit T une variable aléatoire telle que $T(\Omega) = \mathbb{N}$ et telle que $\mathbb{E}(Tg(T)) = \lambda\mathbb{E}(g(T+1))$ pour toute fonction g de $\mathbb{N}$ dans $\mathbb{N}$ telle que $\mathbb{E}(g(T+1)) < +\infty$. Montrer que T suit une loi de Poisson.

IX.24 Loi Zéta ★★

[Corrigé]

Soit $s > 1$ un nombre réel et soit X une variable aléatoire à valeurs dans $\mathbb{N}^*$ dont la loi est donnée par :

$\forall n \in \mathbb{N}^*,\ \mathbb{P}(X = n) = \dfrac{\lambda}{n^s}$ pour un certain réel λ. On pose $\zeta(s) = \displaystyle\sum_{n=1}^{+\infty} \frac{1}{n^s}$. Si $n \in \mathbb{N}^*$, on note $\{n|X\}$ l'événement "n divise X" et $\{n \nmid X\}$ l'événement complémentaire. Enfin on note $(p_n)_{n\in\mathbb{N}^*}$ la suite strictement croissante des nombres premiers.

1. Que vaut λ ?
2. Calculer $\mathbb{P}(n|X)$ pour $n \in \mathbb{N}^*$.
3. Soit $(\alpha_i)_{i\in\mathbb{N}^*}$ une suite d'entiers naturels. Montrer que les événements $\{p_1^{\alpha_1}|X\}, \{p_2^{\alpha_2}|X\}, \dots$ sont mutuellement indépendants.
4. Soit $r \geq 1$ un entier. Montrer que $\mathbb{P}\left(\displaystyle\bigcap_{i=1}^{r}\{p_i \nmid X\}\right) = \displaystyle\prod_{i=1}^{r}(1 - p_i^{-s})$.
5. En déduire que $\zeta(s)^{-1} = \displaystyle\lim_{n\to+\infty} \prod_{k=1}^{n} \left(1 - p_k^{-s}\right)$.
6. Est-ce que la famille $\left(\dfrac{1}{p}\right)_{p\in\mathcal{P}}$, où $\mathcal{P}$ désigne l'ensemble des nombres premiers, est sommable ?

IX.25 Taux de panne ★★

[Corrigé]

Soient $(\Omega, \mathcal{A}, \mathbb{P})$ un espace probabilisé et X une variable aléatoire définie sur Ω et à valeurs dans $\mathbb{N}^*$ vérifiant : $\forall n \in \mathbb{N}^*,\ \mathbb{P}(X \geq n) > 0$.

On définit le *taux de panne* de X par la suite $(x_n)_{n\geq 1}$ avec : $x_n = \mathbb{P}(X = n|X \geq n)$.

1. Montrer que si l'on pose $\mathbb{P}(Y = n) = \dfrac{1}{n(n+1)}$ pour tout $n \in \mathbb{N}^*$, on définit une loi de probabilité. Déterminer le taux de panne de Y.
2. Dans le cas général, établir que $\forall n \geq 2,\ \mathbb{P}(X \geq n) = \displaystyle\prod_{k=1}^{n-1}(1 - x_k)$.
3. En déduire une expression de $\mathbb{P}(X = n)$ en fonction des x_k valable pour tout $n \geq 1$.
4. Déterminer les variables aléatoires discrètes à taux de panne constant.

IX.26 Matrice aléatoire (1) ★★

[Corrigé]
Soient X_1 et X_2 des variables aléatoires indépendantes suivant une même loi géométrique de paramètre $p \in]0,1[$. On pose

$$A = \begin{pmatrix} X_1 & 1 \\ 0 & X_2 \end{pmatrix}$$

1. Montrer que A est presque sûrement inversible.
2. Trouver la probabilité pour que A soit diagonalisable.

IX.27 Matrice aléatoire (2)

[Corrigé]
Soient $\lambda > 0$ et Y une variable aléatoire à valeurs dans $\mathbb{Z}$ tels que :

— $\forall n \in \mathbb{N},\ \mathbb{P}(Y = n) = \mathbb{P}(Y = -n)$;

— $|Y| \sim \mathcal{P}(\lambda)$

On pose $A = \begin{pmatrix} 0 & Y & 1 \\ Y & 0 & 1 \\ Y & 1 & 0 \end{pmatrix}$

1. Donner la loi de $\mathrm{rg}(A)$.
2. Calculer la probabilité que A soit diagonalisable.

IX.28 Matrice aléatoire (3)

[Corrigé]
Soient X, Y, Z, T des variables aléatoires i.i.d. de loi de Benoulli $\mathcal{B}(p)$. On pose :

$$A = \begin{pmatrix} X & X & X & X \\ X & Y & Y & Y \\ X & Y & Z & Z \\ X & Y & Z & T \end{pmatrix}$$

1. Donner la loi de $\mathrm{Tr}(A)$
2. Calculer la probabilité que A soit inversible.
3. Calculer la probabilité que A soit diagonalisable.

IX.29 Matrice aléatoire (4)

[Corrigé]
Soient $\lambda > 0$, X et Y deux variables aléatoires i.i.d. de loi $\mathcal{P}(\lambda)$.
On pose $A = \begin{pmatrix} (-1)^X & 1 \\ (-1)^Y & 1 \end{pmatrix}$

1. Calculer la probabilité que A soit inversible.
2. Calculer la probabilité que A soit diagonalisable.

IX.30 Matrice aléatoire (5)

[Corrigé]
Soient $p, q \in]0,1[$ et X, Y deux variables aléatoires telles que $X \sim \mathcal{G}(p)$ et $Y \sim \mathcal{G}(q)$.
On pose $A = \begin{pmatrix} X & -Y \\ Y & -X \end{pmatrix}$ Calculer la probabilité que A soit diagonalisable.

IX.31 Matrice aléatoire (6)

[Corrigé]
Soit p un nombre premier et $X_0, \dots, X_{p-1}$ des variables aléatoires i.i.d. de loi $\mathcal{B}\left(\frac{1}{2}\right)$. On pose :

$$A = \begin{pmatrix} X_0 & X_1 & \cdots & X_{p-1} \\ X_{p-1} & X_0 & \cdots & X_{p-2} \\ \vdots & \vdots & \ddots & \vdots \\ X_1 & X_2 & \cdots & X_0 \end{pmatrix}$$

Quelle est la probabilité que A soit inversible ?

IX.32 Matrice aléatoire (7)

[Corrigé]
Soit $M \in \mathcal{M}_n(\mathbb{C})$ une matrice aléatoire dont les coefficients sont choisis uniformément dans $\{0,1\}$. Montrer que la probabilité que M soit inversible est minorée par une constante indépendante de n.

IX.33 Matrice de Rademacher

[Corrigé]
Une variable aléatoire X suit une loi de Rademacher si $X(\Omega) = \{-1,1\}$ et $\mathbb{P}(X = -1) =$

$\mathbb{P}(X=1)=\dfrac{1}{2}$. Soit $M=(X_{ij})_{1\leq i,j\leq n}$ une matrice aléatoire telle que les X_{ij} suivent des lois de Rademacher mutuellement indépendantes. On note p_n la probabilité que les colonnes de M forment une base orthogonale de $\mathcal{M}_{n,1}(\mathbb{R})$.
Montrer qu'il existe une suite $(\varepsilon_n)_{n\in\mathbb{N}}$ de limite nulle et $N\in\mathbb{N}$ tels que $\forall n\geq N,\ p_n\leq e^{-n}\sqrt{2\pi n}(1+\varepsilon_n)$.

IX.34 Vecteur propre aléatoire ★★★

[Corrigé]
Soient $A=\begin{pmatrix}0&-1&0\\2&1&-2\\1&-1&1\end{pmatrix}$ et $U=\begin{pmatrix}X\\Y\\Z\end{pmatrix}$ avec X,Y,Z trois variables aléatoires indépendantes, X et Z suivant $\mathcal{G}(p)$ avec $p\in]0,1[$ et Y suivant $\mathcal{P}(\lambda)$ avec $\lambda\in\mathbb{R}_+^*$.
Déterminer la probabilité que U soit un vecteur propre de A.

IX.35 Equation différentielle à coefficients aléatoires

[Corrigé]
Soient A,B,C trois variables aléatoires i.i.d. suivant une loi de Poisson de paramètre $\lambda>0$. On considère l'équation différentielle $Ay''+By'+Cy=0$.
Montrer que la probabilité $p(\lambda)$ que les solutions de cette équation différentielle s'annulent une infinité de fois tend vers 1 pour $\lambda\to+\infty$.

IX.36 Série entière aléatoire

[Corrigé]
Soit $(X_n)_{n\in\mathbb{N}}$ une suite de variable aléatoire i.i.d. suivant une loi géométrique de paramètre p. Que peut-on dire du rayon de convergence de la série entière $\sum_{n\in\mathbb{N}}X_nz^n$?

IX.37 Permutation aléatoire

[Corrigé]
Soient $X_1,\dots,X_{n-1}$ des variables aléatoires mutuellement indépendantes telles que $\forall i\in[\![1;n-1]\!],\ X_i\sim\mathcal{U}([\![i;n]\!])$. Déterminer la loi de la permutation aléatoire :

$$(n,X_n)\circ\cdots\circ(1,X_1)$$

IX.38 Permutations composées d'un grand cycle

[Corrigé]
Soit $n \in \mathbb{N}^*$. Soit σ une variable aléatoire suivant la loi uniforme sur $\mathcal{S}_{2n}$. On note p_n la probabilité que σ ait dans sa décomposition en cycles à supports disjoints un cycle de longueur supérieure ou égale à n. Montrer que $(p_n)_{n\in\mathbb{N}^*}$ converge et calculer sa limite.

IX.39 Loi conjointe (1) ★★

[Corrigé]
Soient X et Y deux variables aléatoires à valeurs dans $\mathbb{N}$ et $p \in]0,1[$.
On suppose que la loi conjointe de X et Y vérifie :

$$\mathbb{P}(X=k,Y=n) = \begin{cases} \binom{n}{k} a^n p(1-p)^n & \text{si } k \leq n \\ 0 & \text{sinon} \end{cases} \text{ avec } a \in \mathbb{R}.$$

1. Déterminer la valeur de a.
2. Déterminer la loi marginale de Y.
3. Sachant que : $\forall x \in]-1,1[$, $\displaystyle\sum_{n=k}^{+\infty} \binom{n}{k} x^{n-k} = \frac{1}{(1-x)^{k+1}}$,
   Reconnaître la loi de X.
4. Les variables X et Y sont-elles indépendantes ?

IX.40 Loi conjointe (2) ★★★

[Corrigé]
Soient $n \in \mathbb{N}$ et X et Y deux variables aléatoires à valeurs dans $[\![0;n]\!]$. On pose $\mathbb{P}(X=i,Y=j) = \lambda\binom{n}{i}\binom{n}{j}$ pour $(i,j) \in [\![0;n]\!]^2$.

1. Déterminer λ.
2. Donner les lois marginales de X et Y.
3. X et Y sont-elles indépendantes ?
4. On considère la matrice $B = (\mathbb{P}(X=i,Y=j))_{0\leq i,j\leq n}$. Expliciter B, puis calculer B^p pour $p \in \mathbb{N}^*$.
5. B est-elle diagonalisable ? Déterminer ses valeurs propres et les sous-espaces propres associés.

IX.41 Fonction caractéristique ★★

[Corrigé]
On appelle *Fonction caractéristique* d'une variable aléatoire X prenant des valeurs dans $\mathbb{Z}$, l'application $\varphi_X : \mathbb{R} \to \mathbb{C}$ donnée par $\varphi_X(t) = \mathbb{E}(e^{itX})$

1. Vérifier que φ_X est définie, continue sur $\mathbb{R}$ et 2π-périodique.
2. On suppose que X admet une espérance. Vérifier que φ_X est de classe $\mathcal{C}^1$ sur $\mathbb{R}$ et exprimer $\mathbb{E}(X)$ à l'aide de φ'_X.
3. On suppose X admet également une variance. Vérifier que φ_X est de classe $\mathcal{C}^2$ sur $\mathbb{R}$ et exprimer $\mathbb{V}(X)$ à l'aide des dérivées de φ_X.

IX.42 Fonction génératrice des moments ★★★★★

[Corrigé]
Soit X une variable aléatoire discrète réelle. On note I_X l'ensemble des $t \in \mathbb{R}$ pour lesquels la variable e^{tX} admet une espérance finie et l'on pose

$$M_X(t) = \mathbb{E}(e^{tX}) \text{ pour tout } t \in I_X$$

1. Montrer que I_X est un intervalle contenant 0.
2. On suppose que 0 est intérieur à I_X. Montrer que la variable aléatoire X admet un moment à tout ordre (c'est à dire que X^n est d'espérance finie quel que soit $n \in \mathbb{N}$) et que, sur un intervalle centré en 0,

$$M_X(t) = \sum_{n=0}^{+\infty} \frac{\mathbb{E}(X^n)}{n!} t^n$$

IX.43 Inégalité de Jensen ★

[Corrigé]
Soient $f : \mathbb{R} \to \mathbb{R}$ une fonction dérivable et convexe ainsi que X une variable aléatoire réelle admettant une espérance finie.

1. Montrer que $f(X) \geq f(\mathbb{E}(X)) + f'(\mathbb{E}(X))(X - \mathbb{E}(X))$.
2. En déduire que si $f(X)$ admet une espérance finie alors $\mathbb{E}(f(X)) \geq f(\mathbb{E}(X))$.

IX.44 Inégalité de Hölder ★★

[Corrigé]
Soient $p, q \in]1, +\infty[$ tels que $\dfrac{1}{p} + \dfrac{1}{q} = 1$.

1. Montrer que $\forall x, y \in \mathbb{R}_+,\ xy \leq \dfrac{x^p}{p} + \dfrac{y^q}{q}$.
2. Soient X, Y deux variables aléatoires réelles positives d'espérance finies. Montrer que :
$$\mathbb{E}(XY) \leq \mathbb{E}(X^p)^{1/p}\mathbb{E}(Y^q)^{1/q}$$
On pourra commencer par traiter le cas $\mathbb{E}(X^p) = \mathbb{E}(Y^q) = 1$.
3. Quelle inégalité retrouve-t-on lorsque $p = q = 2$?

IX.45 Modes de convergences ★★★

[Corrigé]
Soit (X_n) une suite de variables aléatoires discrètes réelles sur Ω, $X : \Omega \mapsto \mathbb{R}$ une variable aléatoire discrète.
Convergence en probabilité. On dit que (X_n) converge en probabilité vers X si :
$$\forall \varepsilon > 0\,, \quad \lim_{n\to+\infty} \mathbb{P}(|X_n - X| > \varepsilon) = 0.$$

1. *Convergence presque sûre* On dit que (X_n) converge presque sûrement vers X s'il existe un événement A presque sûr tel que (X_n) converge simplement vers X sur A
   a. Supposons que (X_n) converge presque sûrement vers X. Montrer que (X_n) converge en probabilité vers X.
   b. Supposons que pour tout $\varepsilon > 0$, $\sum \mathbb{P}(|X_n - X| > \varepsilon)$ converge. Montrer que (X_n) converge presque sûrement vers X.
   c. Supposons que (X_n) convergence en probabilité vers X, montrer qu'il existe une sous-suite de (X_n) qui converge presque sûrement vers X.
   d. Montrer que la réciproque de a. est fausse.
   On pourra choisir les X_n indépendants et suivant une loi de Bernoulli de paramètre p_n tel que p_n tend vers 0 et la série de terme général p_n diverge.
2. *Convergence* $\mathcal{L}^1$ Si les X_n et X admettent une espérance, on dit que (X_n) converge dans $\mathcal{L}^1$ vers X quand la suite $(\mathbb{E}(|X_n - X|))_{n\in\mathbb{N}}$ converge vers 0.
Montrer que la convergence dans $\mathcal{L}^1$ implique la converge en probabilité et que la réciproque est fausse.
3. *Convergence en loi* On suppose ici que les X_n et X sont à valeurs dans $\mathbb{Z}$. On dit que (X_n) converge en loi quand vers X si pour tout $k \in \mathbb{Z}$, $\lim_{n\to+\infty} \mathbb{P}(X_n = k) = \mathbb{P}(X = k)$.
Montrer que la convergence en probabilité implique la convergence en loi et que la réciproque est fausse.

IX.46 Marche aléatoire sur $\mathbb{Z}^d$ ★★★

[Corrigé]
Dans les exercices suivant, on s'intéresse à

IX.46.1 Le cas $d = 1$ ★★

On considère une puce se déplaçant sur une droite graduée par les entiers relatifs. Sa position à l'instant initial $t = 0$ est $k = 0$. A chaque instant $t \in \mathbb{N}^*$, elle se déplace aléatoirement de sa position $k \in \mathbb{Z}$ à la position $k+1$ ou $k-1$. Soit $p \in]0,1[$. On définit sur un espace probabilisé $(\Omega, \mathcal{A}, \mathbb{P})$ une suite de variables aléatoires indépendantes et identiquement distribuées $(X_t)_{t\in\mathbb{N}^*}$ dont la loi est définie par :

$$\forall t \in \mathbb{N}^*,\ \mathbb{P}(X_t = 1) = p \text{ et } \mathbb{P}(X_t = -1) = 1 - p.$$

Enfin, pour tout $n \in \mathbb{N}^*$, on pose $S_n = \sum_{t=1}^{n} X_t$.

1. Pour tout $t \in \mathbb{N}^*$, déterminer la loi de la variable aléatoire $Y_t = \dfrac{X_t + 1}{2}$. En déduire que pour tout $n \in \mathbb{N}^*$, la variable aléatoire $\sum_{t=1}^{n} Y_t$ suit une loi binomiale dont on précisera les paramètres.
2. En déduire que pour tout $n \in \mathbb{N}^*$, $\mathbb{P}(S_n = 0) = \begin{cases} \binom{n}{\frac{n}{2}} (p(1-p))^{\frac{n}{2}} & \text{si } n \text{ est pair} \\ 0 & \text{sinon} \end{cases}$
3. Déterminer la limite de la suite $(\mathbb{P}(S_{2n} = 0))_{n\in\mathbb{N}}$ selon les valeurs de p et interpréter le résultat.

On souhaite maintenant savoir combien de fois en moyenne la puce passe par l'origine lors de son parcours. Pour cela, on note pour tout $j \in \mathbb{N}$, O_{2j} la variable aléatoire égale à 1 si la puce est à l'origine à l'instant $t = 2j$, 0 sinon. Pour tout $n \in \mathbb{N}$, on pose $T_n = \sum_{j=0}^{n} O_{2j}$.

4. Soit $j \in \mathbb{N}$. Déterminer la loi de la variable aléatoire O_{2j}. En déduire que :

$$\forall n \in \mathbb{N},\ \mathbb{E}(T_n) = \sum_{j=0}^{n} \binom{2j}{j} (p(1-p))^j$$

5. On suppose dans cette question que $p \neq \dfrac{1}{2}$. Calculer $\lim\limits_{n\to+\infty} \mathbb{E}(T_n)$ et interpréter ce résultat.
6. On suppose dans cette question que $p = \dfrac{1}{2}$. Montrer par récurrence que :

$$\forall n \in \mathbb{N},\ \mathbb{E}(T_n) = \frac{2n+1}{2^{2n}} \binom{2n}{n}$$

En déduire $\lim\limits_{n\to+\infty} \mathbb{E}(T_n)$ et interpréter.

IX.46.2 Le cas $d = 2$

IX.46.3 Le cas général

Remarque : Une marche alétoire sera dite récurrente si et seulement si la propabilité que la particule repasse à l'origine O pour un certain instant t ultérieur fini vaut 1. *Cette propriété de récurrence dépend fortement de la dimension de l'espace, le théorème de Polya énonce que : la marche aléatoire est récurrente si et seulement si $d = 1$ ou $d = 2$.*

IX.47 Matrice de covariances ★★

[Corrigé]

Soient $X_1, \dots, X_n$ des variables aléatoires discrètes réelles de L^2. On appelle *matrice de covariance* du vecteur aléatoire $X = \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$ la matrice :

$$\Sigma = (\mathrm{Cov}(X_i, X_j))_{1 \leq i,j \leq n}$$

1. Soit $A = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in \mathcal{M}_{n,1}(\mathbb{K})$.
   Exprimer la variance de $A^\top X$ en fonction de la matrice Σ et de A.
2. Montrer que Σ est diagonalisable et que ses valeurs propres sont toutes positives
3. Déterminer une condition nécessaire et suffisante pour que Σ soit inversible.
   Remarque : On ne manquera pas de voir la ressemblance entre matrice de covariances et matrice de Gram, la covariance étant quasi assimilable à un produit scalaire.

IX.48 Maximisation de la variance sous contrainte ★★

[Corrigé]

On considère n ampoules s'allumant aléatoirement de manière indépendante, la probabilité que la i-ème s'allume étant de p_i. On note Y la variable aléatoire donnant le nombre d'ampoules qui sont allumées.

1. Donner l'espérance et la variance de Y.
2. On note $m = \mathbb{E}(Y)$. Déterminer, à m fixé, les p_i tels que $\mathbb{V}(Y)$ soit maximale.
   Quelle loi suit Y pour de tels p_i ?

IX.49 Inégalité de Kosmanek ★

[Corrigé]
Soit $(\Omega, \mathcal{P}(\Omega), \mathbb{P})$ un espace probabilisé fini.

1. Soit C un événement. Montrer que $\mathbb{V}(\mathbb{1}_C) \leq \frac{1}{4}$.
2. Soient A et B deux événements. Montrer que $|\operatorname{Cov}(\mathbb{1}_A, \mathbb{1}_B)| \leq \frac{1}{4}$.
3. En déduire que $|\mathbb{P}(A \cap B) - \mathbb{P}(A)\mathbb{P}(B)| \leq \frac{1}{4}$.
   Quand a-t-on égalité ?

IX.50 Inégalité de Cantelli ★★★

[Corrigé]
Soient $\lambda \in \mathbb{R}_+^*$ et X une variable aléatoire réelle discrète possédant un moment d'ordre 2.

1. On suppose que $\mathbb{E}(X) = 0$.
   (a) Montrer que pour tout $u \in \mathbb{R}_+$, $\mathbb{E}((X+u)^2) = \mathbb{V}(X) + u^2$.
   (b) Montrer que pour tout $u \in \mathbb{R}_+$, $\mathbb{P}(X \geq \lambda) \leq \dfrac{\mathbb{V}(X) + u^2}{(\lambda + u)^2}$.
   (c) En déduire que $\mathbb{P}(X \geq \lambda) \leq \dfrac{\mathbb{V}(X)}{\lambda^2 + \mathbb{V}(X)}$.
2. On ne suppose plus maintenant $\mathbb{E}(X) = 0$. Montrer que $\mathbb{P}(X - \mathbb{E}(X) \geq \lambda) \leq \dfrac{\mathbb{V}(X)}{\lambda^2 + \mathbb{V}(X)}$.

IX.51 Inégalité de Hoeffding ★★★

[Corrigé]
On considère une variable aléatoire discrète X centrée et à valeurs dans $[-1, 1]$.

1. Montrer que
$$\forall t \in \mathbb{R}, \forall x \in [-1,1],\ e^{tx} \leq \frac{1}{2}(1-x)e^{-t} + \frac{1}{2}(1+x)e^{t}$$
2. Montrer que
$$\forall t \in \mathbb{R}, \operatorname{ch}(t) \leq e^{\frac{t^2}{2}}$$
3. En déduire que
$$\forall t \in \mathbb{R}, \mathbb{E}(e^{tX}) \leq e^{\frac{t^2}{2}}$$

On considère une variable aléatoire réelle discrète Y.

4. Montrer que
$$\forall t \in \mathbb{R}_+^*, \forall \varepsilon \in \mathbb{R}_+^*, \mathbb{P}(Y \geq \varepsilon) \leq e^{-t\varepsilon}\mathbb{E}(e^{tY})$$

On considère maintenant des variables aléatoires discrètes réelles centrées $X_1, \dots, X_n$ indépendantes telles que $|X_k| \leq c_k$ pour tout $k \in [\![1; n]\!]$ $(c_k > 0)$. On pose $S = \sum_{k=1}^{n} X_k$

5. Montrer que pour tout $\varepsilon \in \mathbb{R}_+^*$,
$$\mathbb{P}(|S| \geq \varepsilon) \leq 2\exp\left(-\frac{\varepsilon^2}{2\sum_{k=1}^{n} c_k^2}\right)$$

IX.52 Théorème d'approximation de Weierstrass ★★★

[Corrigé]
Le but de cet exercice est de démontrer le théorème d'approximation de Weierstrass :
Toute fonction continue sur un segment est limite uniforme sur ce segment de fonctions polynomiales.

Pour tout $n \in \mathbb{N}^*$ on pose pour $k \in [\![0; n]\!]$, $b_k^n(X) = \binom{n}{k} X^k(1-X)^{n-k}$. (Polynômes de Bernstein)
On note $I = [0, 1]$ et on muni $\mathcal{C} = \mathcal{C}^0(I, \mathbb{C})$ de sa norme uniforme.
On définit alors pour tout $f \in \mathcal{C}$ et tout $n \in \mathbb{N}$,
$$B_n(f) : \begin{cases} I & \longrightarrow & \mathbb{C} \\ x & \longmapsto & \sum_{k=0}^{n} f\left(\frac{k}{n}\right) b_k^n(x) \end{cases}$$

Enfin, On fixe $t \in [0, 1]$, on considère une suite de variable aléatoire $(X_n)_{n\in\mathbb{N}^*}$ indépendantes et identiquement distribuées de loi $\mathcal{B}(t)$ et on pose pour tout $n \in \mathbb{N}^*$, $S_n = \sum_{k=1}^{n} X_k$.

1. Soit $n \in \mathbb{N}^*$.
   Justifier qu'il existe une variable aléatoire discrète R_n telle que $B_n(f)(t) = \mathbb{E}(f(R_n))$.
2. Montrer que pour un réel $\delta > 0$ bien choisit,
$$\forall n \in \mathbb{N}^*, \ \mathbb{E}(|f(t) - f(R_n)|) \leq \frac{\varepsilon}{2} + 2||f||_\infty \mathbb{P}(|t - R_n| > \delta)$$
3. Montrer que $\forall n \in \mathbb{N}^*, \ \mathbb{P}(|t - R_n| > \delta) \leq \frac{1}{4n\delta^2}$.

4. Démontrer que $(B_n(f))_{n\in\mathbb{N}^*}$ converge uniformément vers f sur I.
5. En déduire le théorème de d'approximation de Weierstrass.

X Endomorphismes d'un espace euclidien

Dans toute cette section n désigne un entier naturel non nul.

X.1 Equations matricielles ★★

[Corrigé]

1. Existe-t-il deux matrices $A, B \in \mathcal{M}_n(\mathbb{K})$ telles que $AB - BA = I_n$?
2. Existe-t-il une matrice $M \in \mathcal{M}_2(\mathbb{R})$ telle que $M^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$?
3. Existe-t-il une matrice $N \in \mathcal{M}_2(\mathbb{K})$ telle que $N^2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$?

X.2 Equation matricielle faisant intervenir la comatrice ★★★

[Corrigé]
Résoudre dans $\mathcal{M}_n(\mathbb{R})$ l'équation $A = \mathrm{Com}(A)$.

X.3 Matrice de rotation ★★

[Corrigé]
Soient $\mathcal{B}$ une base orthonormée d'un espace euclidien E de dimension 3 ainsi que $u \in \mathcal{L}(E)$

tel que $\mathrm{Mat}_{\mathcal{B}}(u) = \frac{1}{3}\begin{pmatrix} 2 & 2 & 1 \\ -2 & 1 & 2 \\ 1 & -2 & 2 \end{pmatrix}$
Montrer que u est une rotation.
Question Bonus : Donner son axe et son angle.

X.4 Produit mixte et produit vectoriel ★★

[Corrigé]
Soit E un espace euclidien orienté de dimension $n \geq 1$.

1. Soient $\mathcal{B}$ et $\mathcal{B}'$ deux bases orthonormées directes de E. Montrer que $\det_{\mathcal{B}}(\mathcal{B}') = 1$.
2. En déduire que $\det_{\mathcal{B}} = \det_{\mathcal{B}'}$.
3. Soient $x_1, \dots, x_{n-1} \in E^{n-1}$. Montrer que l'application $\varphi : \left\{ \begin{array}{ccc} E & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \det(x_1, \dots, x_{n-1}, x) \end{array} \right.$ est une forme linéaire sur E.
4. En déduire qu'il existe un unique $u \in E$ tel que
$$\forall x \in E, \varphi(x) = \langle x, u \rangle$$

On appelle u le produit vectoriel des vecteurs $x_1, \dots, x_{n-1}$ et on le note $u = x_1 \wedge x_2 \wedge \dots x_{n-1}$.

5. Montrer que l'application
$$(x_1, \dots, x_{n-1}) \in E^{n-1} \mapsto x_1 \wedge x_2 \wedge \cdots \wedge x_{n-1}$$
est une application $(n-1)$-linéaire alternée.

X.5 Hyperplan de $\mathcal{M}_n(\mathbb{K})$ ★★★★

[Corrigé]
Montrer que tout hyperplan de $\mathcal{M}_n(\mathbb{K})$ rencontre $\mathrm{GL}_n(\mathbb{K})$.

X.6 Equation entre projecteurs ★★★

[Corrigé]
Existe-t-il des projecteurs p, q, r d'un espace euclidien E vérifiant $\sqrt{2}p + \sqrt{3}q = r$?

X.7 Exemple de symétrie orthogonale ★

[Corrigé]
Montrer que $s : \left\{ \begin{array}{ccc} \mathcal{M}_n(\mathbb{R}) & \longrightarrow & \mathcal{M}_n(\mathbb{R}) \\ M & \longmapsto & M^\top \end{array} \right.$ est une symétrie orthogonale pour le produit scalaire sur $\mathcal{M}_n(\mathbb{R})$ pour le produit scalaire défini par $\langle A, B \rangle = \mathrm{Tr}(A^\top B)$ pour $A, B \in \mathcal{M}_n(\mathbb{R})$.

X.8 Caractérisations des projections orthogonales ★★

[Corrigé]
Soient E un espace euclidien et p une projection de E. Etablir l'équivalence des trois propriétés suivantes :

— p est orthogonale

— $\forall x, y \in E,\ \langle p(x), y\rangle = \langle x, p(y)\rangle$

— $\forall x \in E,\ \|p(x)\| \leq \|x\|$

X.9 Norme d'une base orthogonale ★★★

[Corrigé]
Soit $(e_1, \dots e_n)$ une base orthogonale de $\mathbb{R}^n$

1. Montrer qu'il existe un vecteur u de $\mathbb{R}^n$ non nul tel que les projetés orthogonaux de $e_1, \dots, e_n$ sur $\text{Vect}(u)$ aient la même norme.
2. Montrer que cette norme commune est indépendante du vecteur u choisi et l'exprimer en fonction de $\|e_1\|, \dots, \|e_n\|$.

X.10 Matrice de Hilbert ★★★

[Corrigé]

1. Montrer que l'application $\langle\ ;\ \rangle : \left\{ \begin{array}{ccc} \mathbb{R}_{n-1}[X]^2 & \longrightarrow & \mathbb{R} \\ (P,Q) & \longmapsto & \displaystyle\int_0^1 P(t)Q(t) \end{array} \right.$ définie un produit scalaire sur $\mathbb{R}_{n-1}[X]$.
2. Montrer que la matrice de Hilbert $H = \left(\frac{1}{i+j+1}\right)_{0\leq i,j\leq n-1} = \begin{pmatrix} 1 & \frac{1}{2} & \cdots & \frac{1}{n} \\ \frac{1}{2} & \frac{1}{3} & \cdots & \frac{1}{n+1} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{n} & \frac{1}{n+1} & \cdots & \frac{1}{2n+1} \end{pmatrix}$ est symétrique réelle définie positive.

X.11 Racine carrée d'un endomorphisme auto-adjoint positif ★★

[Corrigé]

1. Soit f un endomorphisme auto-adjoint positif d'un espace euclidien E. Montrer qu'il existe $g \in \mathcal{S}^+(E)$ tel que $g^2 = f$.
2. Soit f un endomorphisme auto-adjoint défini positif d'un espace euclidien E. Montrer qu'il existe un unique $g \in \mathcal{S}^{++}(E)$ tel que $g^2 = f$.

X.12 Inégalité de convexité ★★

[Corrigé]
Soit $M \in \mathcal{S}_n^+(\mathbb{R})$.
Démontrer que $\dfrac{\mathrm{Tr}(M)}{n} \geq \det(M)^{1/n}$.

X.13 Inégalité à propos des matrices orthogonales ★★★

[Corrigé]
Soit $A \in \mathcal{O}_n(\mathbb{R})$. Montrer que

$$\left|\sum_{1\leq i,j\leq n} m_{i,j}\right| \leq n \leq \sum_{1\leq i,j\leq n} |m_{i,j}| \leq n^{3/2}.$$

X.14 Inégalité de la trace

[Corrigé]
Soient $A, B \in \mathcal{S}_n^+(\mathbb{R})$. Montrer que $0 \leq \mathrm{Tr}(AB) \leq \mathrm{Tr}(A)\,\mathrm{Tr}(B)$.

X.15 Inégalité de Hadamard ★★★

[Corrigé]
Soit $S = (s_{i,j}) \in \mathcal{S}_n^+(\mathbb{R})$. On pourra se servir librement de l'inégalité arithmético-géométrique cf. I-47 tome Analyse.

1. Montrer que $\det(S) \leq \left(\dfrac{1}{n}\mathrm{Tr}(S)\right)^n$.

2. Soient $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{R}^n$, $D = \mathrm{diag}(\alpha_1, \dots, \alpha_n)$ et $S_\alpha = DSD$.
   Vérifier $S_\alpha \in \mathcal{S}_n^+(\mathbb{R})$ et exprimer $\mathrm{Tr}(S_\alpha)$.
3. On suppose S inversible. Vérifier que les coefficients diagonaux de S sont strictement positifs et, en introduisant des réels $\alpha_1, \dots, \alpha_n$ pertinemment choisis, établir que :
$$\det(S) \leq \prod_{i=1}^{n} s_{i,i}$$
4. Justifier que l'inégalité précédente est encore vraie lorsque S n'est pas inversible.

X.16 Perturbations

[Corrigé]

Soit $A \in \mathcal{M}_n(\mathbb{R})$ la matrice Atilla $A = \begin{pmatrix} 1 & \cdots & \cdots & 1 \\ \vdots & \ddots & \iddots & \vdots \\ \vdots & \iddots & \ddots & \vdots \\ 1 & \cdots & \cdots & 1 \end{pmatrix}$.
Quelles sont les matrices $M \in \mathcal{O}_n(\mathbb{R})$ telles que $A + M$ soit inversible ?

X.17 Somme de Cesàro de matrices orthogonales

[Corrigé]
Soit $A \in \mathcal{O}_n(\mathbb{R})$ telle que $-1 \notin \mathrm{Sp}(A)$.

1. Montrer que la suite $\left(\frac{1}{p+1}\sum_{k=0}^{p} A^k\right)_{p\in\mathbb{N}}$ converge et déterminer sa limite.
2. La suite $(A^p)_{p\in\mathbb{N}}$ converge-t-elle ?

X.18 Transformation de Cayley ★★★

[Corrigé]
Soit $A \in \mathcal{A}_n(\mathbb{R})$.

1. Déterminer les valeurs propres possibles de la matrice A.
2. En déduire que les matrices $A + I_n$ et $A - I_n$ sont inversibles.
3. Montrer que la matrice $\Omega = (A + I_n)(A - I_n)^{-1}$ est orthogonale. Et calculer $\det(\Omega)$
4. Démontrer que l'application $\varphi : \left\{ \begin{array}{ccc} \mathcal{A}_n(\mathbb{R}) & \longrightarrow & \{\Omega \in \mathcal{O}_n(\mathbb{R}) | -1 \notin \mathrm{Sp}(\Omega)\} \\ A & \longmapsto & (A + I_n)(A - I_n)^{-1} \end{array} \right.$ est bijective.
5. En déduire que si Ω est une matrice orthogonale et que $-1 \notin \mathrm{Sp}(\Omega)$ alors $\det(\Omega) = 1$. Pouvait-t-on constater cela d'une autre manière ?

X.19 Optimisation (1) ★★

[Corrigé]

Calculer le minimum de $\Phi : \left\{ \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ (a,b) & \longmapsto & \displaystyle\int_0^\pi \left(\sin(x) - ax - bx^2\right)^2 dx \end{array} \right.$.

X.20 Optimisation (2) ★★

[Corrigé]

Déterminer $\inf_{(a,b)\in\mathbb{R}^2} \displaystyle\int_{-\infty}^{+\infty} (t^2 + at + b)^2 e^{-t^2} dt$.

X.21 Optimisation (3)

[Corrigé]

Soient E un espace euclidien et $x_1, \dots, x_p$ des vecteurs de E. Pour $x \in E$, on pose $f(x) = \displaystyle\sum_{i=1}^{p} \|x - x_i\|^2$. Montrer que f atteint son minimum en $m = \dfrac{1}{p}\displaystyle\sum_{i=1}^{p} x_i$.

X.22 Caractérisation des isométries anti-involutives ★★

[Corrigé]

Soient E un espace euclidien et f un endomorphisme de E. Montrer que deux des trois propriétés suivantes entraînent la troisième :

- f est une isométrie vectorielle.
- $f^2 = -\mathrm{Id}_E$
- $f(x)$ est orthogonal à x pour tout $x \in E$.

X.23 Symétrie de l'espace ★★★

[Corrigé]

Soient $a \in \mathbb{R}^*$, u un vecteur unitaire de $\mathbb{R}^3$ munit de sa structure euclidienne usuelle.

1. Montrer que l'application f_a définie par : $f_a(x) = x + a\langle x, u\rangle u$ est un endomorphisme.
2. Montrer qu'il existe un unique $a' \neq 0$ vérifiant : $\forall x \in \mathbb{R}^3, \|f_{a'}(x)\| = \|x\|$.
   Donner la nature de $f_{a'}$ (on pourra s'intéresser à $f_{a'}^2$).
3. Montrer que f_a est un endomorphisme auto-adjoint et déterminer ses éléments propres.

X.24 Réflexion et rotation dans un plan ★★★

[Corrigé]
Soit E un plan orienté.

1. a. Montrer que la composée de deux réflexion du plan E est une rotation.
   b. Justifier que toute rotation peut s'écrire comme le produit de deux réflexion dont l'une peut être choisie arbitrairement.
2. Soient r une rotation et s une réflexion de E.
   Simplifier les composées $s \circ r \circ s$ et $r \circ s \circ r$.
3. A quelle condition peut-on affirmer qu'une rotation et qu'une réflexion commutent.

X.25 Similitude entre matrices orthogonales ★★★

[Corrigé]
Soit $(A, B) \in \mathcal{O}_n(\mathbb{R})^2$.
Montrer que A et B sont semblables si et seulement $\chi_A = \chi_B$.

X.26 Propriété de l'adjoint ★★

[Corrigé]
Soit f un endomorphisme d'un espace euclidien E. Montrer que :

1. $\mathrm{Tr}(f) = \mathrm{Tr}(f^*)$
2. $\det(f) = \det(f^*)$
3. $\chi_f = \chi_{f^*}$
4. $\mathrm{Sp}(f) = \mathrm{Sp}(f^*)$
5. pour tout $\lambda \in \mathrm{Sp}(f), \dim E_\lambda(f) = \dim E_\lambda(f^*)$
6. $\mathrm{rg}(f) = \mathrm{rg}(f^*) = \mathrm{rg}(f \circ f^*) = \mathrm{rg}(f^* \circ f)$.

X.27 Autour de l'adjoint ★★★

[Corrigé]
Soient E un espace euclidien et f un endomorphisme de E tel que $\mathrm{Im}(u) \subset \mathrm{Ker}(u)$.

1. Montrer que $\mathrm{Ker}(f + f^*) = \mathrm{Ker}(f) \cap \mathrm{Ker}(f^*)$.
2. Supposons que $\mathrm{Ker}(u) = \mathrm{Im}(u)$. Montrer que $u + u^*$ est inversible.

X.28 Somme d'une matrice orthogonale et de sa transposée ★★★

[Corrigé]
Soit $A \in \mathcal{M}_n(\mathbb{R})$. Démontrer que les propriétés suivantes sont équivalentes :

— Il existe $B \in \mathcal{O}_n(\mathbb{R})$ telle que $A = B + B^\top$,

— $A \in \mathcal{S}_n(\mathbb{R})$, $\mathrm{Sp}(A) \subset [-2, 2]$ et les valeurs propres de A dans $]-2, 2[$ sont de multiplicité paire.

X.29 Déterminant d'une exponentielle ★

[Corrigé]
Soit $A \in \mathcal{M}_n(\mathbb{K})$.
Montrer que $\det(e^A) = e^{\mathrm{Tr}(A)}$.

X.30 Exponentielle de matrices antisymétriques ★★★

[Corrigé]
Montrer que $\exp : \mathcal{A}_n(\mathbb{R}) \to \mathcal{O}_n(\mathbb{R})$ est une application surjective.

Remarque : La décomposition polaire sur $\mathbb{C}$ est donnée par l'application $\varphi : \begin{cases} \mathbb{R}_+^* \times \mathbb{R} & \longrightarrow & \mathbb{C}^* \\ (r, \theta) & \longmapsto & re^{i\theta} \end{cases}$.
$\exp : \mathcal{A}_n(\mathbb{R}) \to \mathcal{O}_n(\mathbb{R})$ *permet de comprendre d'où vient le nom de décomposition polaire pour les matrice inversible.*

X.31 Théorème spectral ★★★

[Corrigé]
Enoncer et démontrer le théorème spectral.

X.32 Réduction simultanée ★★★★

[Corrigé]
Soient $A \in \mathcal{S}_n^{++}(\mathbb{R})$ et $B \in \mathcal{S}_n^{+}(\mathbb{R})$

1. Montrer qu'il existe $P \in \mathrm{GL}_n(\mathbb{R})$ et $D \in \mathcal{M}_n(\mathbb{R})$ diagonale à coefficients diagonaux strictement positifs telles que :

$$A = P^\top P \quad \text{et} \quad B = P^\top D P$$

2. Montrer que le polynôme $x \mapsto \det(xA - B)$ est scindé sur $\mathbb{R}$
3. Montrer que $\det(A + B) \geq \det(A) + \det(B)$
4. Montrer que $\forall t \in]0, 1[, \det(A)^t \det(B)^{1-t} \leq \det(tA + (1-t)B)$

X.33 Réduction des matrices antisymétriques ★★★★

[Corrigé]
Soit $A \in \mathcal{M}_n(\mathbb{R})$ une matrice antisymétrique.
Montrer que, par le biais d'une matrice de passage orthogonale, la matrice A est semblable à une matrice diagonale par blocs avec sur la diagonale des zéros et/ou différents blocs $M_\alpha = \begin{pmatrix} 0 & -\alpha \\ \alpha & 0 \end{pmatrix}$ avec $\alpha \in \mathbb{R}_+^*$.

X.34 Caractérisation des matrices symétriques positives ★★★

[Corrigé]
On munit $\mathcal{M}_n(\mathbb{R})$ muni de son produit scalaire canonique. On note $\mathcal{A}_n(\mathbb{R})$ l'ensemble des matrices antisymétriques et $\mathcal{S}_n^+(\mathbb{R})$ l'ensemble des matrices symétriques positives.
Soit $A \in \mathcal{M}_n(\mathbb{R})$:

$$\forall U \in \mathcal{O}_n(\mathbb{R}), \quad \mathrm{Tr}(AU) \leq \mathrm{Tr}(A)$$

1. Déterminer le supplémentaire orthogonal de $\mathcal{A}_n(\mathbb{R})$.
2. Soit $B \in \mathcal{A}_n(\mathbb{R})$. Montrer que $\forall x \in \mathbb{R}, \quad \exp(xB) \in \mathcal{O}_n(\mathbb{R})$.
3. Montrer que $A \in \mathcal{S}_n^+(\mathbb{R})$.
4. Etudier la réciproque.

X.35 Matrices entières positives

[Corrigé]
Soient E un ensemble fini et $A_1, \ldots, A_n$ des parties de E. Montrer que $A = (|A_i \cap A_j|)_{1 \leq i,j \leq n}$ est symétrique réelle définie positive.

X.36 Matrices binaires positives

[Corrigé]

1. Déterminer les matrices de $\mathcal{S}_n^{++}(\mathbb{R})$ à coefficients dans $\{0,1\}$.
2. Déterminer les matrices de $\mathcal{S}_n^{+}(\mathbb{R})$ à coefficients dans $\{0,1\}$ et les dénombrer.

X.37 Inégalité de Hoffman-Wielandt ★★★

[Corrigé]

On munit $\mathcal{M}_n(\mathbb{R})$ de la norme euclidienne canonique $\|.\|_F$.
Pour toute matrice symétrique réelle $M \in S_n(\mathbb{R})$, on note $\lambda_1(M) \geq \cdots \geq \lambda_n(M)$ ses valeurs propres rangées dans l'ordre décroissant.
Soient A et B deux matrices de $S_n(\mathbb{R})$.

1. Montrer que, pour tout $M \in \mathcal{M}_n(\mathbb{R})$ et pour tout P et Q dans $\mathcal{O}_n(\mathbb{R})$, on a : $\|PMQ\|_F = \|M\|_F$.
2. On note $D_A = \mathrm{diag}(\lambda_1(A), \ldots, \lambda_n(A))$ et $D_B = \mathrm{diag}(\lambda_1(B), \ldots, \lambda_n(B))$. Montrer qu'il existe une matrice orthogonale $P = (p_{i,j})$ telle que $\|A - B\|_F = \|D_A P - P D_B\|_F$.
3. Montrer que $\|A - B\|_F^2 = \sum_{1 \leq i,j \leq n} p_{i,j}^2 (\lambda_i(A) - \lambda_j(B))^2$

On note $\mathcal{B}_n(\mathbb{R})$ l'ensemble des matrices bistochastiques de $\mathcal{M}_n(\mathbb{R})$.
On pose $f : \left\{ \begin{array}{ccc} \mathcal{M}_n(\mathbb{R}) & \longrightarrow & \mathbb{R} \\ M & \longmapsto & \displaystyle\sum_{1 \leq i,j \leq n} m_{i,j} (\lambda_i(A) - \lambda_j(B))^2 \end{array} \right.$.

4. Justifier que f admet un minimum sur $\mathcal{B}_n(\mathbb{R})$.

On se propose de montrer que ce minimum est atteint en la matrice identité.

5. Soit $(i,j,k) \in [\![1;n]\!]^3$ tel que $j \geq i$ et $k \geq i$. Montrer que, pour $M \in \mathcal{M}_n(\mathbb{R})$ et pour $x \in \mathbb{R}^+$,

$$f(M + xE_{i,i} + xE_{j,k} - xE_{i,k} - xE_{j,k}) - f(M) = 2x(\lambda_i(A) - \lambda_j(A))(\lambda_k(B) - \lambda_i(B)) \leq 0$$

6. Soient $n \geq 2$ et $M = (m_{i,j}) \in \mathcal{B}_n(\mathbb{R})$ une matrice différente de l'identité. On note i le plus petit entier appartenant à $[\![1;n]\!]$ tel que $m_{i,i} \neq 1$. Montrer qu'il existe une matrice $M' = (m'_{i,j}) \in \mathcal{B}_n(\mathbb{R})$ telle que $f(M') \leq f(M)$ et $m_{j,j} = 1$ pour tout $j \in [\![1;n]\!]$.
7. En déduire que $\min\{f(M) | M \in \mathcal{B}_n(\mathbb{R})\} = f(I_n)$.
8. En déduire que $\forall (A,B) \in \mathcal{S}_n(\mathbb{R})^2, \sum_{i=1}^{n} (\lambda_i(A) - \lambda_i(B))^2 \leq \|A - B\|_F^2$.

X.38 Distance aux matrices de rang au plus r

[Corrigé]

On munit $\mathcal{M}_n(\mathbb{R})$ de sa structure euclidienne canonique. Pour tout $r \in [\![0;n]\!]$ on note B_r l'ensemble des matrices de $\mathcal{M}_n(\mathbb{R})$ de rang au plus r.

1. Soit $A \in \mathcal{S}_n(\mathbb{R})$. Montrer que la distance entre A et B_r est atteinte, et la calculer en fonction du spectre de A.
2. Soit $A \in \mathcal{M}_n(\mathbb{R})$. Montrer que la distance entre A et B_r est atteinte, et la calculer en fonction du spectre de A.

X.39 Théorème de Courant-Fischer ★★★

[Corrigé]
Soit u un endomorphisme autoadjoint d'un espace euclidien E de dimension $n \geq 1$ dont le produit scalaire est noté $\langle .,. \rangle$.
On note $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ les valeurs propres de u comptées avec multiplicité, S la sphère unité de E et, pour tout $p \in [\![1;n]\!]$, $\mathcal{F}_p$ l'ensemble de tous les sous-espaces vectoriels de E de dimension p.
Soit $p \in [\![1;n]\!]$. Etablir que :

$$\lambda_p = \sup_{F \in \mathcal{F}_p} \left(\inf_{x \in F \cap S} \langle u(x), x \rangle \right) = \inf_{F \in \mathcal{F}_{n+1-p}} \left(\sup_{x \in F \cap S} \langle u(x), x \rangle \right)$$

X.40 Principe de Ky-Fan

[Corrigé]
Soient E un espace euclidien de dimension n et $u \in \mathcal{S}(E)$. Si V est un sous-espace vectoriel de E, on note $u_V : V \to V$ l'endomorphisme obtenu comme composition de u avec la projection orthogonale sur V. On note $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ les valeurs propres de u comptées avec multiplicité et pour tout $p \in [\![1;n]\!]$, $\mathcal{F}_p$ l'ensemble de tous les sous-espaces vectoriels de E de dimension p.
Etablir que :

$$\forall p \in [\![1;n]\!], \ \sum_{i=1}^{p} \lambda_i = \max_{V \in \mathcal{F}_p} \mathrm{Tr}(u_V)$$

X.41 Théorème de Cartan-Dieudonnée ★★★★

[Corrigé]
Soient E un espace vectoriel euclidien de dimension n et $f \in \mathcal{O}_n(E)$. Notons $F = \ker(f - \mathrm{Id}_E)$ et $p(f) = n - \dim(F)$.
Montrer que f s'écrit comme produit de $p(f)$ réflexions, et qu'on ne peut pas faire moins.
Pour démontrer ce résultat, on pourra procéder par récurrence forte sur $p(f)$.
Par convention, Id_E est le produit de 0 réflexions.
Remarque : L'entier $p(f)$ est appelée *codimension* de l'espace des invariants de f.

X.42 Relation d'ordre des matrices symétriques

[Corrigé]

Soient A et B dans $\mathcal{S}_n(\mathbb{R})$. On dit que $A \leq B$ lorsque $B - A \in \mathcal{S}_n^+(\mathbb{R})$

1. Vérifier qu'il s'agit bien d'une relation d'ordre. La relation d'ordre est-elle totale ?
2. Soient $E = \mathcal{S}_n^{++}(\mathbb{R})$ et $f : \left\{ \begin{array}{ccc} E & \longrightarrow & E \\ A & \longmapsto & A^{-1} \end{array} \right.$
   Montrer que f est décroissante.

XI

Décomposition matricielle

Dans toute cette section n désigne un entier supérieur ou égal à 1.

XI.1 Décomposition de Dunford ★★★

[Corrigé]
Soit $M \in \mathcal{M}_n(\mathbb{C})$. On note pour $\lambda \in \mathrm{Sp}(M)$, $F_\lambda = \mathrm{Ker}(M - \lambda I_n)^{m_\lambda}$, où m_λ désigne la multiplicité de λ en tant que valeur propre de M, le sous-espace caractéristique de M associée à la valeur propre λ.

1. Montrer que $\mathbb{C}^n = \bigoplus_{\lambda \in \mathrm{Sp}(M)} F_\lambda$.
2. Montrer qu'il existe un couple $(D, N) \in \mathcal{M}_n(\mathbb{C})^2$ tel que
   (i) $M = D + N$;
   (ii) D est diagonalisable ;
   (iii) N est nilpotente ;
   (iv) $DN = ND$.
3. On admet qu'un tel couple vérifie $(D, N) \in \mathbb{C}[M]^2$.
   Montrer que ce couple est unique.

On admettra pour les applications qui suivent, si nécessaire, que D et N sont des polynômes en M.

XI.1.1 Diagonalisabilité de l'exponentielle d'une matrice ★★★

Soit $A \in \mathcal{M}_n(\mathbb{C})$. Montrer que $\exp(A)$ est diagonalisable si et seulement si A l'est.

XI.1.2 Surjectivité de l'exponentielle matricielle ★★★★

1. Soit $M \in \mathrm{GL}_n(\mathbb{C})$.
   Démontrer qu'il existe un unique couple $(D, U) \in \mathcal{M}_n(\mathbb{C})^2$ tel que :
   - $M = DU$;
   - D est diagonalisable ;
   - U est unipotente, c'est à dire que $U - I_n$ est nilpotente ;
   - $DU = UD$.
2. Montrer $\exp : \mathcal{M}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ est surjective.

XI.1.3 Opérateur de commutation ★★★

Soit $A \in \mathcal{M}_n(\mathbb{C})$.
On pose $\mathrm{Comm}_A : \left\{ \begin{array}{ccc} \mathcal{M}_n(\mathbb{C}) & \longrightarrow & \mathcal{M}_n(\mathbb{C}) \\ B & \longmapsto & AB - BA \end{array} \right.$.

1. On suppose que A est diagonalisable et on note $A = PDP^{-1}$ avec $D = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$.
   Montrer que Comm_A est diagonalisable.
2. On suppose que Comm_A est diagonalisable. Déterminer la décomposition de Dunford de Comm_A en fonction de celle de A et en déduire que A est diagonalisable.

XI.1.4 Deux applications non continues

Montrer que les applications $\varphi : \left\{ \begin{array}{ccc} \mathcal{M}_n(\mathbb{C}) & \longrightarrow & \mathcal{M}_n(\mathbb{C}) \\ M = D + N & \longmapsto & D \end{array} \right.$ et $\psi : \left\{ \begin{array}{ccc} \mathcal{M}_n(\mathbb{C}) & \longrightarrow & \mathcal{M}_n(\mathbb{C}) \\ M = D + N & \longmapsto & N \end{array} \right.$
ne sont pas continues.

XI.2 Décomposition polaire ★★★

[Corrigé]

1. Soient E un espace euclidien de dimension n et $u \in S^{++}(E)$. Soit $v \in S^{++}(E)$ tel que $v^2 = u$.
   a. Déterminer v.
   b. Montrer que v est un polynôme en u.
2. Soit $A \in \mathrm{GL}_n(\mathbb{R})$.
   a. Montrer que $A^\top A \in S_n^{++}(\mathbb{R})$.
   b. En déduire qu'il existe un unique couple $(O, S) \in \mathcal{O}_n(\mathbb{R}) \times S_n^{++}(\mathbb{R})$ tel que $A = OS$.
3. Soit $A \in \mathcal{M}_n(\mathbb{R})$.
   Montrer qu'il existe un couple $(O, S) \in \mathcal{O}_n(\mathbb{R}) \times S_n^{+}(\mathbb{R})$ tel que $A = OS$. Ce couple est-il unique ?

XI.2.1 Sous-groupe compact maximal de $\mathrm{GL}_n(\mathbb{R})$ ★★★

On munit $\mathbb{R}^n$ de son produit scalaire usuel $\langle\ ,\ \rangle : (X,Y) \mapsto X^\top Y$ et on note $\|.\|_2$ la norme associée. Pour $A \in \mathcal{M}_n(\mathbb{R})$ on note $\rho(A) = \max\{|\lambda|,\ \lambda \in \mathrm{Sp}(A)\}$. On pose $|||.|||_2 : A \in \mathcal{M}_n(\mathbb{R}) \mapsto \sup_{\substack{X\in\mathbb{R}^n \\ \|X\|_2=1}} \|AX\|_2$.

1. Montrer que $\forall A \in \mathcal{M}_n(\mathbb{R}),\ |||A|||_2 = \sqrt{\rho(A^\top A)}$.
2. Montrer que $\mathcal{O}_n(\mathbb{R})$ est un sous-groupe compact de $\mathrm{GL}_n(\mathbb{R})$.
3. Soit G un sous-groupe compact de $\mathrm{GL}_n(\mathbb{R})$ qui contient $\mathcal{O}_n(\mathbb{R})$. On cherche à montrer que $G = \mathcal{O}_n(\mathbb{R})$. Pour cela on fixe $A \in G$ et on note $A = OS$ sa décomposition polaire.
   a. Montrer que les valeurs propres de S sont toutes inférieures à 1.
   b. Montrer que $\mathrm{Sp}(S) = \{1\}$.
4. Conclure.

XI.2.2 Enveloppe convexe des matrices orthogonales ★★★

On pourra librement utiliser dans cet exercice le théorème de projection sur un convexe compact cf. VIII-33 tome Analyse
On munit $\mathcal{M}_{n,1}(\mathbb{R})$ de son produit scalaire usuel $\langle\ ,\ \rangle_2 : (X,Y) \mapsto X^\top Y$. On note $\|.\|_2$ la norme associée à ce produit scalaire.
On munit ensuite $\mathcal{M}_n(\mathbb{R})$ de la norme subordonnée $|||.|||_2 : A \mapsto \sup_{\substack{X\in\mathcal{M}_{n,1}(\mathbb{R}) \\ \|X\|_2=1}} \|AX\|_2$ et on note $\mathcal{B}$ la boule unité fermée de $\mathcal{M}_n(\mathbb{R})$ pour cette norme.

1. Soit $A \in \mathcal{M}_n(\mathbb{R})$. Exprimer $|||A|||_2$ en fonction des valeurs propres de $A^\top A$.
2. Montrer que l'enveloppe convexe (cf. VIII-36 tome Analyse) de $\mathcal{O}_n(\mathbb{R})$ est contenue dans $\mathcal{B}$.
3. On suppose qu'il existe une matrice $M \in \mathcal{B}$ qui n'est pas dans l'enveloppe convexe de $\mathcal{O}_n(\mathbb{R})$. On admet que $\mathrm{Conv}(\mathcal{O}_n(\mathbb{R}))$ est une partie compacte de $\mathcal{M}_n(\mathbb{R})$ (cf. VIII-37 tome Analyse) et on note N le projeté convexe de M sur $\mathrm{Conv}(\mathcal{O}_n(\mathbb{R}))$ pour le produit scalaire $\langle\ ,\ \rangle : (A,B) \in \mathcal{M}_n(\mathbb{R})^2 \mapsto \mathrm{Tr}(A^\top B)$ et on pose $A = (M-N)^\top$. On écrit enfin $A = US$ une représentation polaire de A.
   a. Montrer que $\forall V \in \mathrm{Conv}(\mathcal{O}_n(\mathbb{R})),\ \mathrm{Tr}(AV) \leq \mathrm{Tr}(AN) < \mathrm{Tr}(AM)$.
   b. En déduire que $\mathrm{Tr}(S) < \mathrm{Tr}(USM)$.
   c. Montrer que $\mathrm{Tr}(S) \geq \mathrm{Tr}(MUS)$ puis conclure.

XI.2.3 Points extrémaux des matrices orthogonales ★★★

On munit $\mathcal{M}_{n,1}(\mathbb{R})$ de son produit scalaire usuel $\langle\ ,\ \rangle : (X,Y) \mapsto X^\top Y$. On note $\|.\|_2$ la norme associée à ce produit scalaire.

On munit ensuite $\mathcal{M}_n(\mathbb{R})$ de la norme subordonnée $|||.||| : A \mapsto \sup_{\substack{X\in\mathcal{M}_{n,1}(\mathbb{R})\\ \|X\|_2=1}} \|AX\|_2$ et on note $\mathcal{B}$ la boule unité fermée de $\mathcal{M}_n(\mathbb{R})$ pour cette norme. On dit qu'un élément $A \in \mathcal{B}$ est extrémal dans $\mathcal{B}$ si l'écriture $A = \frac{1}{2}(B+C)$ avec $B, C \in \mathcal{B}$ entraîne $A = B = C$. On cherche à déterminer l'ensemble des points extrémaux de $\mathcal{B}$.

1. Soit $U \in \mathbb{O}_n(\mathbb{R})$ qui s'écrit $U = \frac{1}{2}(V+W)$ avec $V, W \in \mathcal{B}$. Montrer que pour tout $X \in \mathcal{M}_{n,1}(\mathbb{R})$ les vecteurs VX et WX sont liées et en déduire que U est extrémale dans $\mathcal{B}$.

Soit $A \in \mathcal{B}\backslash\mathbb{O}_n(\mathbb{R})$.

2. Montrer que l'on peut écrire $A = PDQ$ avec $P, Q \in \mathbb{O}_n(\mathbb{R})$ et D une matrice diagonale dont les coefficients diagonaux $d_1, \dots, d_n$ sont tous positifs ou nuls.
3. Montrer que $\forall i \in [\![1; n]\!],\ d_i \leq 1$ et que de plus, $\exists j \in [\![1; n]\!],\ d_j < 1$.
4. En déduire l'existence de deux matrices distinctes A_α et $A_{-\alpha}$ de $\mathcal{B}$ telles que $A = \frac{1}{2}(A_\alpha + A_{-\alpha})$. Conclure.

XI.2.4 Matrice extraite d'une matrice orthogonale

Soit $M \in \mathcal{M}_n(\mathbb{R})$. On dit que M a la propriété (P) si et seulement si il existe $U \in \mathbb{O}_{n+1}(\mathbb{R})$ telle que M soit la matrice extraite de U en lui retirant sa dernière ligne et sa dernière colonne i.e :

$$\exists \alpha_1, \dots, \alpha_{2n+1} \in \mathbb{R},\ U = \begin{pmatrix} & & & \alpha_{2n+1} \\ & M & & \vdots \\ & & & \alpha_{n+2} \\ \alpha_1 & \cdots & \alpha_n & \alpha_{n+1} \end{pmatrix} \in \mathbb{O}_{n+1}(\mathbb{R})$$

1. On suppose que $M = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$ est une matrice diagonale. Déterminer une condition nécessaire et suffisante portant sur ses coefficients pour que M ait la propriété (P).
2. On suppose que $M \in \mathcal{S}_n(\mathbb{R})$. Déterminer une condition nécessaire et suffisante pour que M ait la propriété (P).
3. On suppose que $M \in \mathrm{GL}_n(\mathbb{R})$ et on écrit $M = OS$ sa décomposition polaire. Déterminer une condition nécessaire et suffisante portant sur $M^\top M$ pour que M ait la propriété (P).

XI.2.5 Matrices qui respectent le volume de k-parallélépipèdes rectangles

XI.3 Décomposition QR ★★

[Corrigé]

1. Montrer que $\mathcal{O}_n(\mathbb{R})$ et $T_n^{++}(\mathbb{R})$ (ensemble des matrices triangulaires supérieures donc tous les coefficients diagonaux sont strictement positifs) sont des sous-groupes de $(\mathrm{GL}_n(\mathbb{R}), \times)$.
2. Montrer que $\mathcal{O}_n(\mathbb{R}) \cap T_n^{++}(\mathbb{R}) = \{I_n\}$.
3. Soit $A \in \mathrm{GL}_n(\mathbb{R})$. Soit $(e_1, \dots e_n)$ la base constituée des vecteurs colonnes de A.
   Soit $\mathcal{B}_{GS} = (v_1, \dots, v_n)$ la base orthonormée obtenue à partir de $\mathcal{B}$ grâce au procédé d'orthonormalisation de Gramm-Schmidt.
   A l'aide de ces bases, montrer qu'il existe un unique couple de matrices $(Q, R) \in \mathcal{O}_n(\mathbb{R}) \times T_n^{++}(\mathbb{R})$ tel que $A = QR$

XI.3.1 Matrice de Householder

1. Comment s'écrit la réflexion h par rapport à l'hyperplan orthogonal à un vecteur non nul a ?
2. Montrer que sa matrice dans la base canonique est $H = I_n - \dfrac{2[a]^\top [a]}{\|a\|^2}$
3. Montrer que si u et v sont deux vecteurs distincts de $\mathbb{R}^n$ et de même norme, alors il existe une réflexion unique h telle que $h(u) = v$.
4. Etudier l'existence d'une réflexion h transformant un vecteur u de $\mathbb{R}^n$ en $v = \lambda e_1$.
5. Plus généralement, soit i un indice de $[\![1; n]\!]$ et $u = (x_1, \dots, x_n)$. On pose $v = (x_1, \dots, x_{j-1}, \lambda, 0, \dots, 0$ et $w = (0, \dots, 0, x_j, \dots, x_n)$.
   Etudier l'existence d'une réflexion h de $\mathbb{R}^n$ transformant u en v.
   Que dire des vecteurs $e_1, \dots, e_{j-1}$ pour l'application h ?
6. Déduire de ce qui précède qu'il existe $n-1$ matrice de Householder $H_1, H_2, \dots, H_{n-1}$ telles que pour tout j les coefficients sous-diagonaux des j premières colonnes de $A_j = H_j H_{j-1} \dots H_1 A$ soient nuls.
7. Montrer comment des produits successifs par les matrices H_j permettent d'obtenir séparément les composantes Q et R d'une décomposition QR de la matrice A.
8. Illustrer cette méthode en décomposant $A = \begin{pmatrix} -4 & 20 & 35 & 5 \\ -4 & -30 & -15 & 55 \\ -8 & 40 & -80 & -65 \\ 23 & -15 & 30 & 15 \end{pmatrix}$

XI.4 Décomposition LU ★★★

[Corrigé]
Soit $A = (a_{ij})_{1\leq i,j\leq n} \in \mathcal{M}_n(\mathbb{K})$. Pour $k \in [\![1; n]\!]$, on appelle k-ième mineur principal de A le déterminant de la matrice A à laquelle on a supprimé les $n-k$ dernières lignes et colonnes : $\Delta_k = \det(a_{ij})_{1\leq i,j\leq k}$.
Montrer que les propositions suivantes sont équivalentes :

— Les mineurs principaux de A sont tous non nuls

— Il existe une matrice $L = \begin{pmatrix} 1 & 0 & \dots & 0 \\ & 1 & \ddots & \vdots \\ & * & \ddots & 0 \\ & & & 1 \end{pmatrix}$ et une matrice $U = \begin{pmatrix} d_1 & & & \\ 0 & d_2 & * & \\ \vdots & \ddots & \ddots & \\ 0 & \dots & 0 & d_n \end{pmatrix}$ telles que $A = LU$

XI.4.1 $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ ★★

Montrer que l'ensemble des matrices de $\mathcal{M}_n(\mathbb{R})$ (resp. $\mathcal{M}_n(\mathbb{C})$) admettant une composition LU est un ouvert de $\mathcal{M}_n(\mathbb{R})$ (resp. $\mathcal{M}_n(\mathbb{C})$).

XI.4.2 $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$ ★★ (HP)

Soit p un nombre premier.
Dénombrer l'ensemble des matrices de $\mathbb{Z}/p\mathbb{Z}$ qui admettent une décomposition LU.

XI.4.3 Algorithme de calcul ★★

Soit $A \in \mathcal{M}_n(\mathbb{K})$ admettant une décomposition LU.
Proposer des algorithmes python permettant de calculer le déterminant de A, déterminer son inverse, et permettant de résoudre un système du type $AX = Y$ pour $Y \in \mathcal{M}_{n,1}(\mathbb{K})$.
Montrer que la complexité temporelle de l'algorithme de calcul du déterminant est de l'ordre de $\frac{2}{3}n^3$ en comptant seulement le nombre d'additions et de multiplications, pour lesquelles on considérera qu'elle prennent le même temps constant. Commenter.

XI.4.4 Décomposition de Cholesky

Montrer que $S_n^{++}(\mathbb{R}) = \{A^\top A,\ A \in \mathrm{GL}_n(\mathbb{R})\}$.

XI.5 Lemme de Fitting

[Corrigé]

1. Soit E un espace vectoriel de dimension n et $u \in \mathcal{L}(E)$, il existe $p \in \mathbb{N}$ tel que :
$$E = \mathrm{Ker}(u^p) \oplus \mathrm{Im}(u^p).$$
2. Soit $M \in \mathcal{M}_n(\mathbb{K})$ est semblable à une matrice de la forme $\begin{pmatrix} N & 0 \\ 0 & P \end{pmatrix}$ où N est une matrice nilpotente et C est une matrice carrée inversible.

Remarque : A l'aide de ce résultat, on peut calculer le cardinal du cône nilpotent sur un corps fini de cardinal Le cardinal n_d de l'ensemble des matrices carrés nilpotentes de taille d sur un corps de cardinal q est :
$$n_d = q^{d(d-1)}.$$
Il permet également de démontrer le théorème Krull-Schmidt, qui requis des connaissances sur les produits directs de groupes.

XI.6 Réduction de Jordan

[Corrigé]

On appelle bloc de Jordan toute matrice de la forme : $J_n(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \ddots & \vdots \\ 0 & 0 & \lambda & \ddots & 0 \\ \vdots & \vdots & \ddots & \ddots & 1 \\ 0 & 0 & \cdots & 0 & \lambda \end{pmatrix}$

1. Soit $M \in \mathcal{M}_n(\mathbb{K})$ de polynôme caractéristique scindé sur $\mathbb{K}$. On pose pour tout $\lambda \in \mathrm{Sp}(M)$,$F_\lambda = \mathrm{Ker}(M - \lambda I_n)^{m_\lambda}$ Montrer que $\mathcal{M}_{n,1}(\mathbb{K}) = \bigoplus_{\lambda \in \mathrm{Sp}(M)} F_\lambda$
2. Soit $f \in \mathcal{L}(E)$ nilpotent d'indice p. Montrer que pour tout $x \in E$ tel que $f^{p-1}(x) \neq 0$. Montrer que $\mathcal{F} = (f^{p-1}(x), \ldots, f(x), x)$ est libre. Ecrire la matrice de f dans $\mathcal{F}$.
3. Déduire que toute matrice $M \in \mathcal{M}_n(\mathbb{K})$ tel que son polynôme caractéristique est scindé est semblable à une matrice diagonale par blocs de Jordan.

XI.6.1 Application

1. Retrouver le résultat de la décomposition de Dunford

XI.7 Réduction de Frobenius

[Corrigé]

Soient E un espace vectoriel de dimension n, et $u \in \mathcal{L}(E)$. On admettra les résultats sur les polynômes minimaux ponctuels.

En raisonnant par récurrence, montrer qu'il existe une décomposition $E = \bigoplus_{i=1}^{r} E_i$ en sous-espaces stables et $(P_i)_{i\in[\![1;r]\!]} \in \mathbb{K}[X]^r$ tels que :

— $u_{|E_i}$ est un endomorphisme cyclique de polynôme P_i.

— pour tout $i \in [\![1; r-1]\!]$, $P_{i+1}|P_i$ et $P_1 = \pi_u$

De, plus $(P_1, \dots, P_r)$ ne dépend que de u.

XI.7.1 $M \sim M^\top$

Démontrer que toute matrice de $\mathcal{M}_n(\mathbb{K})$ est semblable à sa transposée.

XI.7.2 Matrices semblables à leur inverse

Déterminer les matrices de $\mathrm{GL}_n(\mathbb{K})$ semblables à leur inverse.

XI.7.3 Bicommutant

XII

Divers

XII.1 Fonction $\mathbb{R}$-linéaire mais pas $\mathbb{C}$-linéaire ★

[Corrigé]
Donner un exemple de fonction $\mathbb{R}$-linéaire mais pas $\mathbb{C}$-linéaire.

XII.2 Relation d'ordre ★★

[Corrigé]
Soient D_1 et D_2 deux dés à 6 faces.
On pose X_1 et X_2 les variables aléatoires qui a un lancé des deux dés associe le nombre exhibé sur la face supérieur du dé 1 et du dé 2 respectivement.
On définit alors la relation D_1 est plus faible ($\preceq$) que D_2 par $D_1 \preceq D_2 \iff \mathbb{P}(X_1 > X_2) \geq \mathbb{P}(X_2 > X_1)$.
$\preceq$ est-elle une relation d'ordre ?

XII.3 Ordre lexicographique ★

[Corrigé]
On définit sur $\mathbb{C}$ la relation binaire $\preceq$ par :

$$\forall (z_1, z_2) \in \mathbb{C}^2,\ z_1 \preceq z_2 \iff [\Re(z_1) < \Re(z_2) \text{ ou } (\Re(z_1) = \Re(z_2) \text{ et } \Im(z_1) \leq \Im(z_2))]$$

Montrer que $\preceq$ est une relation d'ordre sur $\mathbb{C}$ et qu'elle n'est pas totale. Que peut-on modifier pour quelle le soit ?

XII.4 Sous-groupes de $\mathrm{GL}_n(\mathbb{C})$ d'exposant fini ★★★★★

[Corrigé]
Soit $n \in \mathbb{N}^*$.
Soit G un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$ tel que

$$\exists k \in \mathbb{N}^*,\ \forall M \in G,\ M^k = I_n$$

Démontrer que G est fini.
On pourra montrer que l'ensemble T des traces des éléments de G est fini puis construire une injection de G dans T^d pour un certain $d \in \mathbb{N}^*$ bien choisi.

XII.5 Formule de Burnside ★★★★

[Corrigé]
Soit V un $\mathbb{K}$-espace vectoriel de dimension $n \in \mathbb{N}^*$.
On se donne G un sous-groupe fini de $\mathrm{GL}(V)$ et on note :

$$V^G = \{x \in V \mid \forall g \in G,\ g(x) = x\}$$

Démontrer que $\dfrac{1}{|G|}\displaystyle\sum_{g\in G} \mathrm{Tr}(g) = \dim(V^G)$.

XII.6 Théorème de Fermat matriciel ★★★ (HP)

[Corrigé]
Soit $p \in \mathbb{N}$ un nombre premier. Soit $M \in \mathcal{M}_n(\mathbb{Z})$.

1. Démontrer que pour tout polynôme $P \in \mathbb{Z}[X]$, on a : $P(X^p) - P(X)^p \in p\mathbb{Z}[X]$.
2. Justifier qu'il existe $A \in \mathcal{M}_n(\mathbb{Z}[X])$ telle que $(XI_n - M)^p - (X^pI_n - M^p) = pA$
3. Démontrer que $\chi_{M^p}(X^p) - \chi_M(X)^p \in \mathbb{Z}[X]$.
4. En déduire que $\mathrm{Tr}(M^p) \equiv \mathrm{Tr}(M)[p]$

XII.7 Développement décimal propre d'un réel ★★★

[Corrigé]

Démontrer que tout réel $x \in [0,1[$ s'écrit de manière unique $x = \displaystyle\sum_{n=1}^{+\infty} \frac{a_n}{10^n}$ avec $(a_n)_{n\in\mathbb{N}^*}$ une suite à valeurs dans $[\![0;9]\!]$ qui ne stationne pas à 9.

XII.7.1 Une caractérisation des rationnels ★★★

Soit $x \in [0,1[$. Montrer que $x \in \mathbb{Q}$ si et seulement si son développement décimal propre est périodique à partir d'un certain rang.

XII.8 Distribution du premier chiffre des puissances de 2 ★★★

[Corrigé]
Soit $i \in [\![1;9]\!]$. On note $N_i(n)$ le nombre d'éléments de $\{2, 2^2, \dots, 2^n\}$ dont le premier chiffre dans l'écriture décimale est i. On note pour $x \in \mathbb{R}$, $\{x\} = x - \lfloor x \rfloor$ la partie fractionnaire de x.

1. Montrer qu'en notant $\theta = \log_{10}(2)$, $N_i(n)$ est exactement le nombre d'entier $k \in [\![1;n]\!]$ tels que $\{k\theta\}$ est dans $[\log_{10}(i), \log_{10}(i+1)[$.
2. Montrer que la suite $(\{k\theta\})_{k\in\mathbb{N}^*}$ est dense dans $[0,1]$.
3. En déduire qu'il existe une infinité de puissances de 2 dont le premier chiffre est i.

XIII

Correction

XIII.1 Correction Algèbre linéaire

XIII.1.1 Extension de corps ★★

[Enoncé]

1. $\mathbb{R}$ est un $\mathbb{R}$-espace vectoriel de $\mathbb{C}$ qui est un $\mathbb{C}$-espace vectoriel. De plus $\mathbb{R}$ n'est pas un $\mathbb{C}$-espace vectoriel de $\mathbb{C}$ puisque $i \times 1_{\mathbb{C}} = i \neq \mathbb{R}$ par exemple.
2. Soit $(v_1, \dots, v_n)$ une base du $\mathbb{C}$-espace vectoriel V. Soit $v \in V$.

   $\exists (z_1, \dots, z_n) \in \mathbb{C}^n,\ v = \sum_{k=1}^{n} z_k v_k$.

   Posons pour tout $k \in [\![1; n]\!]$, $x_k = \mathrm{Re}(z_k)$, $y_k = \mathrm{Im}(z_k)$ et $w_k = iv_k \in V$ car V est un $\mathbb{C}$-espace vectoriel.

   On peut alors écrire v comme combinaison linéaire à coefficients réels de $v_1, \dots, v_n, w_1, \dots, w_n$:

   $$v = \sum_{k=1}^{n} x_k v_k + y_k w_k$$

   ce qui justifie que V est un $\mathbb{R}$-espace vectoriel et que $\mathcal{F} = (v_1, \dots, v_n, w_1, \dots, w_n)$ en est une partie génératrice.

   De plus, si $a_1, \dots, a_n, b_1, \dots, b_n$ sont des réels vérifiant $\sum_{k=1}^{n} a_k v_k + b_k w_k = 0_V$ alors $\sum_{k=1}^{n} (a_k + ib_k) v_k = 0_V$.

   On en déduit, comme $(v_1, \dots, v_n)$ est une famille libre du $\mathbb{C}$-espace vectoriel V, que $\forall k \in [\![1; n]\!],\ a_k + ib_k = 0$.

   Puis comme a_k et b_k sont des réels, $a_k = b_k = 0$ quel que soit $k \in [\![1; n]\!]$.

   Ainsi $\mathcal{F}$ est une base du $\mathbb{R}$-espace vectoriel V qui est donc de dimension $2n$.

3. Supposons (i).
Montrons que $(\mathbb{M}, +, \times)$ est un $\mathbb{L}$-espace vectoriel de dimension finie : $\forall(\alpha, \beta) \in \mathbb{L}^2,\ \forall(x, y) \in \mathbb{M}^2$,
   — $(\mathbb{M}, +)$ est un groupe abélien.
   — $(\alpha + \beta) \times x = \alpha \times x + \beta \times x$;
   — $\alpha \times (x + y) = \alpha \times x + \alpha \times y$;
   — $(\alpha \times \beta) \times x = \alpha \times (\beta \times x)$;
   — $\mathbb{1}_{\mathbb{L}} \times x = x$.

   et que $\mathbb{L}$ est un sous-espace vectoriel de $\mathbb{M}$:
   — $\mathbb{L} \subset \mathbb{M}$;
   — $0_{\mathbb{M}} = 0_{\mathbb{L}} \in \mathbb{L}$;
   — $\forall(g_1, g_2, \lambda) \in \mathbb{L} \times \mathbb{K},\ g_1 - \lambda g_2 \in \mathbb{L}$.

   Donc $\mathbb{L}$ est de dimension finie en tant que $\mathbb{K}$-espace vectoriel.
   On se donne une base $(f_1, \dots, f_k)$ de $\mathbb{M}$ sur $\mathbb{L}$ et une base $(g_1, \dots, g_p)$ de $\mathbb{L}$ sur $\mathbb{K}$. Soit $f \in \mathbb{M}$.
   $\exists(\lambda_1, \dots, \lambda_k) \in \mathbb{L}^k,\ f = \sum_{i=1}^{k} \lambda_i f_i$.
   $\forall i \in [\![1; k]\!],\ \exists(\mu_{i,1}, \dots, \mu_{i,p}) \in \mathbb{K}^p,\ \lambda_i = \sum_{j=1}^{p} \mu_{i,j} g_j$.
   Posons pour $(i, j) \in [\![1; k]\!] \times [\![1; p]\!],\ h_{i,j} = g_j f_i \in \mathbb{M}$.
   On a $f = \sum_{\substack{1 \leq i \leq k \\ 1 \leq j \leq p}} \mu_{i,j} h_{i,j}$ donc $\mathcal{F} = (h_{i,j})_{\substack{1 \leq i \leq k \\ 1 \leq j \leq p}}$ est une famille génératrice du $\mathbb{K}$-espace vectoriel $\mathbb{M}$.
   De plus, si $(\eta_{i,j})_{\substack{1 \leq i \leq k \\ 1 \leq j \leq p}} \in \mathbb{K}^{kp}$ vérifie $\sum_{\substack{1 \leq i \leq k \\ 1 \leq j \leq p}} \eta_{i,j} h_{i,j} = 0$ alors,

$$\sum_{i=1}^{k} \left(\sum_{j=1}^{p} \eta_{i,j} g_j \right) f_i = 0$$

   d'où par liberté de $(f_1, \dots, f_k)$,

$$\forall i \in [\![1; k]\!],\ \sum_{j=1}^{p} \eta_{i,j} g_j = 0$$

   Puis par liberté de $(g_1, \dots, g_p)$,

$$\forall(i, j) \in [\![1; k]\!] \times [\![1; p]\!],\ \eta_{i,j} = 0$$

   Par conséquent $\mathcal{F}$ est une base du $\mathbb{K}$-espace vectoriel $\mathbb{M}$ et $m = kp$.

Réciproquement supposons (ii).
On note comme précédemment $(f_1, \dots, f_k)$ une base de $\mathbb{M}$ sur $\mathbb{L}$ et $(g_1, \dots, g_p)$ une base de $\mathbb{L}$ sur $\mathbb{K}$. On pose ensuite pour tout $(i,j) \in [\![1;k]\!] \times [\![1;p]\!]$, $h_{i,j} = f_i g_j$ et $\mathcal{F} = (h_{i,j})_{\substack{1 \leq i \leq k \\ 1 \leq j \leq p}}$.
Alors comme $\mathbb{M}$ est un corps, $\text{Vect}_{\mathbb{K}}(\mathcal{F}) \subset \mathbb{M}$. Et si on fixe $f \in \mathbb{M}$ alors,
on sait qu'il existe des éléments $\lambda_1, \dots, \lambda_k \in \mathbb{L}$ tels que $f = \sum_{i=1}^{k} \lambda_i f_i$.
Puis on sait que pour chaque $i \in [\![1;k]\!]$, il existe des éléments $\mu_{i,1}, \dots, \mu_{i,p} \in \mathbb{K}$ tels que $\lambda_i = \sum_{j=1}^{p} \mu_{i,j} g_j$.
Par conséquent $f = \sum_{i=1}^{k} \left(\sum_{j=1}^{p} \mu_{i,j} g_j \right) f_i = \sum_{\substack{1 \leq i \leq k \\ 1 \leq j \leq p}} \mu_{i,j} h_{i,j}$ et $\mathbb{M} \subset \text{Vect}_{\mathbb{K}}(\mathcal{F})$.
On montre comme précédemment que $\mathcal{F}$ est une famille libre et finalement $\mathbb{M} = \text{Vect}_{\mathbb{K}}(\mathcal{F})$ est un $\mathbb{K}$-espace vectoriel de dimension kp.

XIII.1.2 Passage du complexe au réel

[Enoncé]

XIII.1.3 Dimension de $\mathbb{R}$ en tant que $\mathbb{Q}$-espace vectoriel ★★

[Enoncé]

1. On sait que $\mathbb{R}$ est un $\mathbb{R}$-espace vectoriel et comme $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$ on vérifie aisément les axiomes (cf. I.1).
2. Soient $p_1, \dots, p_n$ des nombres premiers distincts et soient $\alpha_1, \dots, \alpha_n$ des nombres rationnels tels que $\sum_{i=1}^{n} \alpha_i \ln(p_i) = 0$.
   On note $I = \{i \in [\![1;n]\!],\ \alpha_i \neq 0\}$ et pour tout $i \in I$, $\alpha_i = \dfrac{a_i}{b_i}$ avec $a_i \in \mathbb{Z}\backslash\{0\}$ et $b_i \in \mathbb{N}^*$.
   Enfin on note pour tout $i \in I$, $c_i = a_i \prod_{j=1}^{n} b_j \in \mathbb{Z}$
   En multipliant par $\prod_{j=1}^{n} b_j$ on a $\sum_{i \in I} c_i \ln(p_i) = 0$ puis $\sum_{\substack{i \in I \\ c_i > 0}} c_i \ln(p_i) = \sum_{\substack{i \in I \\ c_i < 0}} -c_i \ln(p_i)$.
   Ou encore $\ln\left(\prod_{\substack{i \in I \\ c_i > 0}} p_i^{c_i} \right) = \ln\left(\prod_{\substack{i \in I \\ c_i < 0}} p_i^{-c_i} \right)$ c'est à dire $\prod_{\substack{i \in I \\ c_i > 0}} p_i^{c_i} = \prod_{\substack{i \in I \\ c_i < 0}} p_i^{-c_i}$.
   Par unicité de la décomposition en produit de facteurs premiers et comme $\{i \in I,\ c_i >$

$0\} \cap \{i \in I,\ c_i < 0\} = \emptyset$, $\forall i \in I,\ c_i = 0$. Donc $\forall i \in I,\ a_i = 0$ et $\forall i \in [\![1; n]\!],\ \alpha_i = 0$.
Ainsi $(\ln(p_1), \dots, \ln(p_n))$ est $\mathbb{Q}$-libre.

3. On sait qu'il existe une infinité de nombres premiers donc $\mathbb{R}$ n'admet pas de famille $\mathbb{Q}$-libre maximale : $\mathbb{R}$ est un $\mathbb{Q}$-espace vectoriel de dimension infinie.

XIII.1.4 Indépendance des fonctions

[Enoncé]

XIII.1.5 L'ordre a son importance

[Enoncé]
Il est clair que si M est une homothétie alors

$$\forall A, B \in \mathcal{M}_n(\mathbb{R}), \mathrm{Tr}(MAB) = \mathrm{Tr}(MBA)$$

Réciproquement, supposons que M vérifie la propriété de l'énoncé.
Alors elle est vérifié en particulierr pour les matrices élémentaires, cela va nous fournir des conditions très restrictives sur les coefficients de M.
On en déduit que M est une homothétie.

XIII.1.6 Centre de $\mathcal{M}_n(\mathbb{K})$ ★★

[Enoncé]
Soit $A \in Z$. On note pour $1 \leq i, j \leq n,\ E_{ij}$ la matrice dont tous les coefficients sont nuls sauf celui sur la i-ième ligne, j-ième colonne qui vaut 1. Fixons $(i, j) \in [\![1; n]\!]^2$.
$AE_{ij} = E_{ij}A$ donc pour $(k, l) \in [\![1; n]\!]^2$ on a :

$$(AE_{ij})_{kl} = \sum_{p=1}^{n} A_{kp} (E_{ij})_{pl} = A_{ki} (E_{ij})_{il} = (E_{ij})_{kj} A_{jl} = \sum_{p=1}^{n} (E_{ij})_{kp} A_{pl} = (E_{ij}A)_{kl}$$

En particulier, pour $k = i, l = j$ on obtient $A_{ii} = A_{ii} (E_{ij})_{ij} = (E_{ij})_{ij} A_{jj} = A_{jj}$.
Et pour $k \neq i, l = j$ on obtient $A_{ki} = A_{ki} (E_{ij})_{ij} = (E_{ij})_{kj} A_{jj} = 0$.
Ainsi $A = A_{11} I_n$ est une matrice scalaire.

Réciproquement fixons $\alpha \in \mathbb{K}$.
$\forall B \in \mathcal{M}_n(\mathbb{K}),\ (\alpha I_n)B = \alpha B = B(\alpha I_n)$.
Finalement, les seules matrices qui commutent avec toutes les autres sont les matrices scalaires : $Z = \mathrm{Vect}(I_n)$.

XIII.1.7 Racine carrée de la dérivation ★★★

[Enoncé]
Supposons qu'il existe un tel endomorphisme δ. Alors $\delta \circ \Delta = \delta^3 = \Delta \circ \delta$.

Donc $\mathrm{Ker}(\Delta) = \mathrm{Vect}(x \mapsto 1)$ est stable par δ, autrement dit l'image par δ d'une fonction constante est une fonction constante. Intéressons nous à l'image de la fonction constante égale à 1. Si $\delta(x \mapsto 1) = x \mapsto \lambda \neq 0_E$ alors par linéarité $\Delta(x \mapsto 1) = \delta^2(x \mapsto 1) = \delta(x \mapsto \lambda) = \lambda\delta(x \mapsto 1) = x \mapsto \lambda^2 \neq 0_E$ ce qui est absurde.
Par conséquent $\delta(x \mapsto 1) = 0_E$ Mais alors, $\Delta(\delta(\mathrm{Id}_\mathbb{R})) = \delta(\Delta(\mathrm{Id}_\mathbb{R})) = \delta(x \mapsto 1) = 0_E$.
Par conséquent $\delta(\mathrm{Id}_\mathbb{R})$ est une fonction constante d'où $\Delta(\mathrm{Id}_\mathbb{R}) = \delta(\delta(\mathrm{Id}_\mathbb{R})) = 0$ ce qui est absurde.
Ainsi il n'existe pas d'endomorphisme δ de E qui vérifie $\delta^2 = \Delta$.

XIII.1.8 Produit de matrices nilpotentes ★★★★★

[Enoncé]
Montrons le lemme suivant : si A est une matrice non nulle et B est une matrice nilpotente qui commute avec A alors $\mathrm{rg}(AB) < \mathrm{rg}(A)$.
Soient $A \in \mathcal{M}_n(\mathbb{K})\backslash\{0_n\}$ et $B \in \mathcal{M}_n(\mathbb{K})$ une matrice nilpotente qui commute avec A. Posons φ_A et φ_B les endomorphismes canoniquement associés à A et B respectivement.
Il est clair que $\mathrm{Im}(AB) \subset \mathrm{Im}(A)$ donc $\mathrm{rg}(AB) \leq \mathrm{rg}(A)$. Supposons par l'absurde que $\mathrm{rg}(AB) = \mathrm{rg}(A)$
Soit $Y \in \mathrm{Im}(A)$. $\exists X \in \mathcal{M}_{n,1}(\mathbb{K}),\ Y = AX$. Donc $BY = BAX = ABX \in \mathrm{Im}(A)$. Ainsi φ_B induit un endomorphisme $\tilde{\varphi}_B$ sur $\mathrm{Im}(A)$.
De plus, si $Y \in \mathrm{Ker}(\tilde{\varphi}_B)$ alors $BY = 0$ et il existe $X \in \mathcal{M}_{n,1}(\mathbb{K})$ telle que $Y = AX$. Autrement dit $BAX = 0$ ou encore $X \in \mathrm{Ker}(BA) = \mathrm{Ker}(AB)$. Or $\mathrm{Ker}(A) \subset \mathrm{Ker}(AB)$ et on a supposé que $\mathrm{rg}(AB) = \mathrm{rg}(A)$. Donc à l'aide du théorème du rang on en déduit que $\mathrm{Ker}(AB) = \mathrm{Ker}(A)$. Mais alors $Y = 0$ d'où $\tilde{\varphi}_B$ est injectif et donc bijectif.
Pourtant, on montre aisément que $\forall p \in \mathbb{N}^*, \forall X \in \mathcal{M}_{n,1}(\mathbb{K})\ \varphi_B^p(X) = B^pX$. Par conséquent $\tilde{\varphi}_B$ est nilpotent en tant que restriction d'une application nilpotente ; il ne peut pas être bijectif.
En outre, $\mathrm{rg}(AB) < \mathrm{rg}(A)$.
Par récurrence immédiate sur le nombre de matrice dans le produit on en déduit que $\mathrm{rg}\left(\prod_{i=1}^{n} N_i\right) = 0$ c'est à dire que $\prod_{i=1}^{n} N_i = 0$.

XIII.1.9 Suites périodiques ★★★★

[Enoncé]
$(0)_{n\in\mathbb{N}} \in E$ car la suite nulle est 1-périodique par exemple. Soit $(u_n)_{n\in\mathbb{N}}$ une suite p-périodique et $(v_n)_{n\in\mathbb{N}}$ une suite q-périodique pour un certain couple $(p,q) \in (\mathbb{N}^*)^2$. Fixons $\lambda \in \mathbb{C}$.
Par récurrence immédiate, si a est un multiple de p et si b est un multiple de q alors $\forall n \in \mathbb{N},\ u_{n+a} = u_n, v_{n+b} = v_n$.
Notons $m = \mathrm{ppcm}(p,q)$. Comme m est un multiple de p et de q, $\forall n \in \mathbb{N},\ u_{n+m} + \lambda v_{n+m} = u_n + \lambda v_n$.
Autrement dit $(u_n + \lambda v_n)_{n\in\mathbb{N}}$ est m-périodique.

Ainsi E est un sous-espace vectoriel de $\mathbb{C}^{\mathbb{N}}$.
Posons $S : \begin{cases} \mathbb{C}^{\mathbb{N}} & \longrightarrow & \mathbb{C}^{\mathbb{N}} \\ (u_n)_{n\in\mathbb{N}} & \longmapsto & (u_{n+1})_{n\in\mathbb{N}} \end{cases}$. On vérifie que S est un endomorphisme de $\mathbb{C}^{\mathbb{N}}$.
On remarque que $u \in E \iff \exists r \in \mathbb{N}^*,\ S^r(u) = u$.
De plus pour un entier $r \in \mathbb{N}^*$ fixé, $X^r - 1 = \prod_{k=1}^{r}(X - \omega_r^k)$ en notant $\omega_r = e^{\frac{2i\pi}{r}}$.
Enfin pour $1 \leq k_1 \neq k_2 \leq r, (X - \omega_r^{k_1}) \wedge (X - \omega_r^{k_2}) = 1$.
Par conséquent d'après le lemme des noyaux, $\operatorname{Ker}(S^r - \operatorname{Id}_{\mathbb{C}^{\mathbb{N}}}) = \bigoplus_{k=1}^{r} \operatorname{Ker}(S - \omega_r^k \operatorname{Id}_{\mathbb{C}^{\mathbb{N}}})$.
On sait que $\operatorname{Ker}(S - \omega_r^k \operatorname{Id}_{\mathbb{C}^n}) = \{(u_n) \in \mathbb{C}^{\mathbb{N}} \mid \forall n \in \mathbb{N},\ u_{n+1} = \omega_r^k u_n\} = \operatorname{Vect}\left((\omega_r^{kn})_{n\in\mathbb{N}}\right)$. On remarque enfin que $\forall (k, r, p) \in (\mathbb{N}^*)^3,\ (\omega_{pr}^{pkn})_{n\in\mathbb{N}} = (\omega_r^{kn})_{n\in\mathbb{N}}$ ce qui permet de se contenter des $(\omega_r^{kn})_{n\in\mathbb{N}}$ pour r et k premiers entre eux.
On a alors montré que $E = \operatorname{Vect}\left((\omega_r^{kn})_{n\in\mathbb{N}},\ r \wedge k = 1\right)$. Cette famille est bien libre puisqu'elle est formée de vecteurs propres de S associés à des valeurs propres différentes (ce qui est assuré par le fait que k et r sont pris premiers entre eux).

XIII.1.10 Dimension du commutant (1)

[Enoncé]

1. Soit $v, w \in \mathcal{L}(E)$ et $\lambda \in \mathbb{C}$.

$$f_u(v + \lambda w) = u \circ (v + \lambda w) - (v + \lambda w) \circ u = f_u(v) + \lambda f_u(w)$$

   Donc f_u est linéaire.
   On remarque que $\mathcal{C}(u)$ est le noyau de f_u. Donc $\mathcal{C}(u)$ est un sous-espace vectoriel de $\mathcal{L}(E)$.

2.

XIII.1.11 Etude de la comatrice ★★★

[Enoncé]

1. Si $r = n$ alors $J_r = I_n$. On sait que $I_n \operatorname{Com}(I_n)^\top = \det(I_n) I_n$ i.e $\operatorname{Com}(I_n)^\top = I_n$ ou encore $\operatorname{Com}(I_n) = I_n$. Dans ce cas $\operatorname{rg}(\operatorname{Com}(J_r)) = n$.
   Si $r = n - 1$ alors $J_r = \left(\begin{array}{ccc|c} & & & 0 \\ & I_{n-1} & & \vdots \\ & & & 0 \\ \hline 0 & \cdots & 0 & 0 \end{array}\right)$. Le seul mineur non nul de J_r est celui obtenu en retirant la dernière ligne et la dernière colonne de J_r. Le cofacteur associée vaut $(-1)^{2n} \det(I_{n-1}) = 1$ d'où $\operatorname{Com}(J_{n-1}) = J_1$ est de rang 1.

Enfin si $0 \leq r \leq n-2$ alors par définition du rang toute matrice extraite de J_r de taille $n-1$ n'est pas inversible. La comatrice de J_r est donc nulle et est de rang nul.

2. Soit $(A,B) \in \mathcal{M}_n(\mathbb{K})^2$.
Si A et B sont inversibles on sait que AB l'est aussi d'où :
$\mathrm{Com}(AB) = \det(AB)\left((AB)^{-1}\right)^\top = \det(A)\det(B)\left(B^{-1}A^{-1}\right)^\top = \det(A)\left(A^{-1}\right)^\top \det(B)\left(B^{-1}\right)^\top =$
$\mathrm{Com}(A)\,\mathrm{Com}(B)$.
Or on sait (cf. VIII-53 tome Analyse) que $\mathrm{GL}_n(\mathbb{K})$ est dense dans $\mathcal{M}_n(\mathbb{K})$ donc il existe deux suites de matrices inversibles $(A_k)_{k\in\mathbb{N}},\ (B_k)_{k\in\mathbb{N}}$ telles que $A_k \underset{k\to+\infty}{\longrightarrow} A$ et $B_k \underset{k\to+\infty}{\longrightarrow} B$.
De plus, on sait que la fonction $(M,N) \in \mathcal{M}_n(\mathbb{K})^2 \mapsto MN$ est continue car bilinéaire et que la fonction $M \in \mathcal{M}_n(\mathbb{K}) \mapsto \det(M) = \sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma)\prod_{i=1}^{n} m_{i,\sigma(i)}$ est continue car polynomiale en les coefficients de M, d'où $\varphi : M \in \mathcal{M}_n(\mathbb{K}) \mapsto \mathrm{Com}(M)$ est continue car les coefficients de $\mathrm{Com}(M)$ sont polynomiaux en ceux de M (ce sont des calculs de déterminant à la multiplication par un scalaire près).
Par conséquent, par composition et produit de limites, $\mathrm{Com}(A_kB_k) \underset{k\to+\infty}{\longrightarrow} \mathrm{Com}(AB)$ et $\mathrm{Com}(A_k)\,\mathrm{Com}(B_k) \underset{k\to+\infty}{\longrightarrow} \mathrm{Com}(A)\,\mathrm{Com}(B)$.
D'autre part, $\forall k \in \mathbb{N},\ \mathrm{Com}(A_kB_k) = \mathrm{Com}(A_k)\,\mathrm{Com}(B_k)$. Ainsi par unicité de la limite, $\mathrm{Com}(AB) = \mathrm{Com}(A)\,\mathrm{Com}(B)$.

3. Soit $A \in \mathcal{M}_n(\mathbb{K})$. On note $r = \mathrm{rg}(A)$. On sait qu'il existe deux matrices inversibles P, Q telles que $A = PJ_rQ$.
D'après la question précédente, $\mathrm{Com}(A) = \mathrm{Com}(P)\,\mathrm{Com}(J_r)\,\mathrm{Com}(Q)$. Or d'après la question 1, $\mathrm{Com}(P)$ et $\mathrm{Com}(Q)$ sont inversibles car P et Q sont inversibles. Ainsi $\mathrm{Com}(A)$ est équivalente à $\mathrm{Com}(J_r)$, elles ont donc le même rang.
On a alors d'après la question 1 :
$$\mathrm{rg}(\mathrm{Com}(A)) = \begin{cases} 0 & \text{si } r < n-1 \\ 1 & \text{si } r = n-1 \\ n & \text{si } r = n \end{cases}$$

4. Si $n \geq 3$ alors φ n'est pas injective puisque $\varphi(0) = 0 = \varphi(J_1)$. Elle n'est pas non plus surjective car aucune matrice de l'image de φ n'est de rang 2.
Si $n = 1$ alors φ est la fonction constante égale à la matrice (1). Elle n'est donc ni injective ni surjective encore une fois.
Enfin si $n = 2$ alors $\varphi : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$. On remarque alors que $\varphi^2 = \mathrm{Id}_{\mathcal{M}_2(\mathbb{K})}$ donc φ est bijective.
Déterminons $\mathrm{Im}(\varphi)$ dans le cas $\mathbb{K} = \mathbb{C}$. On vient de voir que si $n = 1$ alors $\mathrm{Im}(\varphi) = \{I_1\}$ et si $n = 2$ alors $\mathrm{Im}(\varphi) = \mathcal{M}_2(\mathbb{C})$. Supposons maintenant $n \geq 3$.
On a vu que $\mathrm{Im}(\varphi) \subset \mathrm{GL}_n(\mathbb{C}) \cup \{A \in \mathcal{M}_n(\mathbb{C}),\ \mathrm{rg}(A) = 1\}$.
Fixons $A \in \mathrm{GL}_n(\mathbb{C})$.
$\mathrm{Com}(M) = A \implies \det(\mathrm{Com}(M)^\top) = \det(A^\top) \implies \det(\det(M)M^{-1}) = \det(A) \implies$

$\det(M)^{n-1} = \det(A)$.
On sait qu'il existe $z \in \mathbb{C}$ tel que $z^{n-1} = \det(A)$. On pose donc $M = z\left(A^{-1}\right)^\top$.
On vérifie que $\mathrm{Com}(M)^\top = \det(M)M^{-1} = \dfrac{z^n}{\det(A)} \cdot \dfrac{A^\top}{z} = \dfrac{z^{n-1}}{\det(A)}A^\top = A^\top$ d'où $\mathrm{Com}(M) = A$.
Fixons $A \in \mathcal{M}_n(\mathbb{C})$ de rang 1. $\exists P, Q \in \mathrm{GL}_n(\mathbb{C}),\ A = PJ_1Q$. On rappelle que $J_1 = \mathrm{Com}(J_{n-1})$ et d'après ce qui précède, il existe deux matrices inversibles P', Q' telles que $P = \mathrm{Com}(P')$ et $Q = \mathrm{Com}(Q')$. Donc $A = \mathrm{Com}(P')\,\mathrm{Com}(J_1)\,\mathrm{Com}(Q')$ et d'après la question 2, $A = \mathrm{Com}(P'J_1Q')$.
Par suite, $\mathrm{Im}(\varphi) = \mathrm{GL}_n(\mathbb{C}) \cup \{A \in \mathcal{M}_n(\mathbb{C}),\ \mathrm{rg}(A) = 1\}$.

XIII.1.12 Lemme de Schur

[Enoncé]
Soient $x_1, x_2 \in E$. D'après l'hypothèse de l'énoncé, il existe $\lambda_1, \lambda_2 \in \mathbb{K}$ tel que $u(x_1) = \lambda_1 x_1$ et $u(x_2) = \lambda_2 x_2$.

— Supposons que (x_1, x_2) est une famille libre.
Il existe $\lambda \in \mathbb{K}$ tel que $u(x_1 + x_2) = \lambda(x_1 + x_2)$.
On a par linéarité de u : $u(x_1 + x_2) = \lambda_1 x_1 + \lambda_2 x_2$. Et puisque (x_1, x_2) est une famille libre, $\lambda = \lambda_1 = \lambda_2$.

— Supposons que (x_1, x_2) est une famille liée. Donc il existe $\alpha \in \mathbb{K}$ tel que $x_1 = \alpha x_2$.
$\lambda_1 x_1 = u(x_1) = u(\alpha x_2) = \alpha u(x_2) = \alpha\lambda_2 x_2 = \lambda_2 x_1$.

On en déduit que : u est bien une homothétie.

XIII.1.13 Espaces engendrés par les matrices inversibles et orthogonales

[Enoncé]

XIII.1.14 Espace engendré par les matrices nilpotentes

[Enoncé]

XIII.1.15 Transmission d'information ★★★

[Enoncé]
Supposons que $(A, B) \neq (0, 0)$. Alors on peut se donner $x \in \mathcal{M}_{n,1}\backslash\mathrm{Ker}(A)$ et $y \in \mathrm{Im}(B)\backslash\{0\}$.
On complète la famille (y) en une base $(y, e_2, \ldots, e_n)$ de $\mathcal{M}_{n,1}(\mathbb{K})$.
On définit la matrice carré X en posant $Xy = x$ et $Xe_i = 0$ pour $i \in [\![2; n]\!]$.
Alors pour $z \in \mathcal{M}_{n,1}(\mathbb{K})$ telle que $Bz = y$ on a : $AXBz = AXy = Ax \neq 0$. Donc $AXB \neq 0$.

XIII.1.16 Condition nécessaire et suffisante pour que l'image et le noyau soient supplémentaires

[Enoncé]
On montre aisément que :

$$\mathrm{Ker}(f) \subset \mathrm{Ker}(f^2) \quad \text{et} \quad \mathrm{Im}(f^2) \subset \mathrm{Im} f$$

Montrons que (i)$\Longrightarrow$(ii)
Soit $y \in \mathrm{Im}(f)$
IL existe $x \in E$ tel que $f(x) = y$.
D'après (i), il existe $(x_1, x_2) \in \mathrm{Im}(f) \times \mathrm{Ker}(f)$.
Ainsi $f(x_1) = y$.
Puisque $x_1 \in \mathrm{Im}(f)$, il existe $y' \in E$ tel que $x_1 = f(y')$ donc $f^2(y') = y$.
Donc $\mathrm{Im}(f^2) = \mathrm{Im}(f)$ par double inclusion.
Montrons que (ii)$\Longrightarrow$(iii).
D'après le théorème du rang, $\dim(\mathrm{Ker}(f)) = n - \dim(\mathrm{Im}(f)) = n - \dim(\mathrm{Im}(f^2)) = \dim(\mathrm{Ker}(f^2))$
Et puisque $\mathrm{Ker}(f) \subset \mathrm{Ker}(f^2)$, on en déduit que : $\mathrm{Ker}(f) = \mathrm{Ker}(f^2)$.
Montrons que (iii)$\Longrightarrow$(i)
Soit $x \in \mathrm{Ker}(f) \cap \mathrm{Im}(f)$
$f(x) = 0$
$\exists y \in E, f(y) = x$
Ainsi, $f^2(y) = 0$. Donc $y \in \mathrm{Ker}(f^2) = \mathrm{Ker}(f)$. Ce qui implique que $f(y) = 0$. Donc $x = 0$.
Par conséquent, $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$ sont en somme directe.
De plus, d'après le théorème du rang : $\dim(\mathrm{Im}(f)) + \dim(\mathrm{Ker}(f)) = n$.
Donc $\mathrm{Im}(f) \oplus \mathrm{Ker}(f) = E$.

XIII.1.17 Théorème de Maschle

[Enoncé]

1. a. Soit p un projecteur.
   On sait que $\mathrm{Im}(p) \bigoplus \mathrm{Ker}(p) = \mathcal{M}_n(\mathbb{R})$.
   On remarque que la matrice de p dans une base adaptée à $\mathrm{Im}(p) \bigoplus \mathrm{Ker}(p)$ est J_r où $r = \mathrm{rg}(p)$.
   Ainsi, on en déduit ainsi que : $\mathrm{rg}(p) = \mathrm{Tr}(p)$.

   b. φ_h est clairement un application de G dans G. Et on remarque que φ_h est inversible d'inverse $\varphi_{h^{-1}}$.

2. a.

$$\begin{aligned} p^2 &= \frac{1}{n^2}\sum_{g\in G}\sum_{h\in G} h\circ g \\ &= \frac{1}{n^2}\sum_{g\in G}\sum_{h\in G} g && \text{d'après la question 1b} \\ &= \frac{1}{n^2} n \sum_{g\in G} g \\ &= p \end{aligned}$$

Donc p est un projecteur.

b. Par linéarité de la trace,

$$\mathrm{Tr}(p) = \frac{1}{n}\sum_{g\in G}\mathrm{Tr}(g)$$

Montrons que $\mathrm{Ker}(p - Id_E) = \bigcap_{g\in G}\mathrm{Ker}(g - Id_E)$.

On remarque que $p - Id_E = \dfrac{1}{n}\displaystyle\sum_{g\in G}(g - Id_E)$. Ainsi,

$$\bigcap_{g\in G}\mathrm{Ker}(g - Id_E) \subset \mathrm{Ker}(p - Id_E)$$

Réciproquement soit $x \in \mathrm{Im}(p)$ et soit $g_0 \in G$.

$$g_0(x) = g_0(p(x)) = g_0\left(\frac{1}{n}\sum_{g\in G} g\right) = \frac{1}{n}\sum_{g\in G} g_o \circ g$$

Or d'après la question 1b, φ_{g_0} est une permutation de G, alors

$$g_0(x) = p(x) = x$$

Donc

$$\mathrm{Im}(p) = \mathrm{Ker}(p - Id_E) = \bigcap_{g\in G}\mathrm{Ker}(g - Id_E)$$

Ainsi, d'après la question 1a, on a

$$\dim\left(\bigcap_{g\in G}\mathrm{Ker}(g - Id_E)\right) = \frac{1}{n}\sum_{g\in G}\mathrm{Tr}(g)$$

3. On pose $p = \dfrac{1}{n}\displaystyle\sum_{g\in G} g^{-1}\circ q \circ g$.

Montrons que p est un projecteur.

Puisque pour tout $g \in G$ stabilise F, on en déduit que p est à valeur dans F.
Soit $x \in F$. On a $g(x) \in F$ donc $(p(g(x))) = g(x)$. Donc

$$g^{-1} \circ q \circ g(x) = g^{-1} \circ g(x) = x$$

Par conséquent, p agit comme identité sur F.
Ainsi, p est un projecteur sur F.
Maintenant, montrons que $S = \text{Ker}(p)$ vérifie les propriétés demandées.
D'après les propriétés des projecteurs,

$$S \bigoplus F = E$$

Montrons que S est stable par tous les éléments de G.
On montre d'abord que pour tout $h \in G$, on a :

$$h \circ p \circ h^{-1} = p$$

$$\begin{aligned} h^{-1} \circ p \circ h &= \frac{1}{n} \sum_{g \in G} h^{-1} \circ g^{-1} \circ p \circ g \circ h \\ &= \frac{1}{n} \sum_{g \in G} g \circ p \circ g^{-1} && \text{d'après la question 1b} \\ &= p \end{aligned}$$

Ainsi, pour tout $x \in S$ et pour tout $g \in G$

$$p(g(x)) = g(p(x)) = g(0) = 0$$

Donc $g(x) \in S$.
Donc S est stable par tous les éléments de G.

XIII.2 Correction Réduction géométrique

XIII.2.1 Matrices de rang 1

[Enoncé]

Réduction des matrices de rang 1

1. Soit $M \in \mathcal{M}_n(\mathbb{K})$.
$$\begin{aligned} & \operatorname{rg}(M) = 1 \\ \text{ssi} \quad & \exists (x_1, \dots, x_n) \in \mathbb{R}^n, \exists U \in \mathcal{M}_{n,1}(\mathbb{K}) \text{ tel que } M = (x_1 U | \dots | x_n U) \\ \text{ssi} \quad & \exists (U, V) \in \mathcal{M}_{n,1}(\mathbb{K}) \text{ tel que } M = UV^\top \end{aligned}$$

2. Puisque m est de rang 1, on en déduit qu'il existe $(U, V) \in \mathcal{M}_{n,1}(\mathbb{K})^2$ tel que $M = UV^\top$.
On remarque que $\operatorname{Tr}(M) = V^\top U$. Ainsi, on a aisément $M^2 = \operatorname{Tr}(M)M$

3. Soit $M \in \mathcal{M}_n(\mathbb{K})$ tq $\operatorname{rg}(M) = 1$
Donc d'après le théorème du rang, on a : $\dim(\operatorname{Ker}(M)) = n - 1$.
On en déduit que la multiplicité algébrique de 0 est au moins $n-1$ càd $m_0(M) \geq n-1$.
Donc $X^{n-1} | \chi_M$ et puisque $\deg(\chi_M) = n$, il existe $\alpha \in \mathbb{K}$ tel que $\chi_M = X^{n-1}(X - \alpha)$.
Notons également que $\alpha = \operatorname{Tr}(M)$ car la trace de M est la somme des valeurs M.

   — Si $\operatorname{Tr}(M) = 0$, on a $m_0(M) > n - 1$ donc M n'est pas diagonalisable.

   — Si $\operatorname{Tr}(M) \neq 0$, $m_0(M) = n - 1$ et $\dim(E_{\operatorname{Tr}(M)}(M) = 1 = m_{\operatorname{Tr}(M)}(M)$. Donc M est diagonalisable.

   On conclut donc que M est diagonalisable ssi $\operatorname{Tr}(M) \neq 0$.

4. Soit $A \in \mathcal{M}_3(\mathbb{C})$ tel que $A^3 = \begin{pmatrix} 1 & -2 & 1 \\ 1 & -2 & 1 \\ 1 & -2 & 1 \end{pmatrix} = M$
M est de rang 1 ainsi on a : $M^2 = \operatorname{Tr}(M)M = 0_3$ car $\operatorname{Tr}(M) = 0$.
Donc $A^6 = 0$.
Ainsi A est nilpotente, donc d'après le théorème de Cayley-Hamilton, $A^3 = 0_3$.
Donc il n'y a pas de solution à l'équation : $A^3 = M$.

Diagonalisabilité d'une matrice

Pour tout $\lambda \in \mathbb{R}$, $\chi_M = \det(\mathrm{diag}(\lambda - a_1 + b_1, \dots, \lambda - a_n + b_n) - N)$ avec $N = \begin{pmatrix} b_1 & b_2 & \dots & b_{n-1} & b_n \\ b_1 & b_2 & \ddots & \vdots & \vdots \\ \vdots & b_2 & \ddots & b_{n-1} & b_n \\ \vdots & \vdots & \ddots & b_{n-1} & b_n \\ b_1 & b_2 & \dots & b_{n-1} & b_n \end{pmatrix}$

On remarque que $\mathrm{rg}(N) = 1$ et que $N = UV^\top = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}^\top$. Ainsi, d'après le lemme du déterminant, on a :

$$\chi_M(\lambda) = \det(\mathrm{diag}(\lambda - a_1 + b_1, \dots, \lambda - a_n + b_n)) - V^\top \mathrm{Com}(\mathrm{diag}(\lambda - a_1 + b_1, \dots, \lambda - a_n + b_n))U$$

On choisit λ tel que $\mathrm{diag}(\lambda - a_1 + b_1, \dots, \lambda - a_n + b_n)$ est inversible. Donc :

$$\begin{aligned}\chi_M(\lambda) &= \det(\mathrm{diag}(\lambda - a_1 + b_1, \dots, \lambda - a_n + b_n)) \cdot \left(1 - V^\top \mathrm{diag}\left(\left(\frac{1}{\lambda - a_1 + b_1}, \dots, \frac{1}{\lambda - a_n + b_n}\right)\right) U\right. \\ &= \prod_{i=1}^{n} (\lambda - a_i + b_i)\left(1 - \sum_{i=1}^{n} \frac{b_i}{\lambda - a_i + b_i}\right) \\ &= \prod_{i=1}^{n} (\lambda - a_i + b_i) - \sum_{i=1}^{n} b_i P_i(\lambda)\end{aligned}$$

Avec $P_i(\lambda) = \prod_{j \in [\![1;n]\!], j \neq i} (\lambda - a_i + b_i)$.
Puisque $a_1 \leq \dots \leq a_n$ et $0 < b_n < \dots < b_1$, on a $a_1 - b_1 < \dots < a_n - b_n$.
On a $\chi_M(a_i - b_i) = -b_i \prod_{j \in [\![1;n]\!], j \neq i} [(a_i - b_i) - (a_j - b_j)]$.
Ainsi, $\mathrm{sgn}(\chi_M(a_i - b_i)) = (-1)^{n+1-i}$ et $\lim_{\lambda \to +\infty} \chi_M(\lambda) = +\infty$.
Par conséquent, d'après le théorème des valeurs intermédiaires, pour tout $i \in [\![1;n]\!]$, il existe $\mu_i \in]a_i - b_i, a_{i+1} - b_{i+1}[$ tel que $\chi_M(\mu_i) = 0$ et il existe $\mu_n \in]a_n - b_n, +\infty[$ tel que $\chi_M(\mu_n) = 0$.
On a donc trouvé n racines distinctes de χ_M qui est de degré n. Donc χ_M est scindé à racines simples et par suite M est diagonalisable.

XIII.2.2 Matrices réelles semblables

[Enoncé]
D'après l'énoncé, il existe $P \in GL_n(\mathbb{C})$ tel que $A = PBP^{-1}$. On note $P = S + iR$ avec $(S, R) \in \mathcal{M}_n(\mathbb{R})$. Donc $A(S + iR) = (S + iR)B$, et ainsi par unicité de la partie réelle et

imaginaire, on a : $\begin{cases} AS = SB \\ AR = BR \end{cases}$
De plus, on pose $f : t \mapsto \det(S+tR)$. f est une fonction polynomiale non nulle car $f(i) \neq 0$. Donc il existe $\lambda \in \mathbb{R}$ tel que $f(\lambda) \neq 0$ et donc $S + \lambda R$ est inversible.
Ainsi comme $AS = SB$ et $AR = RB$, on a $A(S + \lambda R) = (S + \lambda R)B$ d'où le résultat.

XIII.2.3 Complément de Schur

[Enoncé]

1. On remarque que : $\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} A^{-1} & -A^{-1}B \\ 0 & I_q \end{pmatrix} = \begin{pmatrix} I_p & 0 \\ CA^{-1} & D - CA^{-1}B \end{pmatrix}$. Donc $\det(M)\det(A^{-1}$ $det(S)$ et donc $\det(M) = \det(A)\det(S)$.
2. Puisque $\begin{pmatrix} A^{-1} & -A^{-1}B \\ 0 & I_q \end{pmatrix}$ est inversible. On en déduit que $\operatorname{rg}(M) = \operatorname{rg}\begin{pmatrix} I_p & 0 \\ CA^{-1} & D - CA^{-1}B \end{pmatrix}$.
   Soit $\begin{pmatrix} X \\ Y \end{pmatrix} \in \operatorname{Ker}\begin{pmatrix} I_p & 0 \\ CA^{-1} & D - CA^{-1}B \end{pmatrix}$ On a : $\begin{cases} X = 0 \\ CX + SY = 0 \end{cases}$
   Par conséquent, $\dim\left(\operatorname{Ker}\begin{pmatrix} I_p & 0 \\ CA^{-1} & D - CA^{-1}B \end{pmatrix}\right) = \dim(\operatorname{Ker}(S)) = q - \operatorname{rg}(S)$ donc $\dim(\operatorname{Ker}(M)) = q - \operatorname{rg}(S)$. Finalement, $\operatorname{rg}(M) = p + q - \dim(\operatorname{Ker}(M)) = p + \operatorname{rg}(S) = \operatorname{rg}(A) + \operatorname{rg}(S)$.

XIII.2.4 Produit de Kronecker

[Enoncé]

1. On a $A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{pmatrix}$ et $C \otimes D = \begin{pmatrix} c_{11}D & c_{12}D \\ c_{21}D & c_{22}D \end{pmatrix}$. Un calcul par blocs donne
   $(A\otimes B)\cdot(C\otimes D) = \begin{pmatrix} (a_{11}c_{11} + a_{12}c_{21})BD & (a_{11}c_{12} + a_{12}c_{22})BD \\ (a_{21}c_{11} + a_{22}c_{21})BD & (a_{21}c_{12} + a_{22}c_{22})BD \end{pmatrix} = \begin{pmatrix} ac_{11}BD & ac_{12}BD \\ ac_{21}BD & ac_{22}BD \end{pmatrix} = (AC$
   en notant ac_{ij} le coefficient en position (i, j) de la matrice AC.
2. $I_2 \otimes B = \begin{pmatrix} B & 0_2 \\ 0_2 & B \end{pmatrix}$ donc $\det(I_2 \otimes B) = (\det B)^2$.
   Soit u l'endomorphisme de C^4 canoniquement associé à $A \otimes I_2$. Notons (e_1, e_2, e_3, e_4) la base canonique de C^4. Alors la matrice de u dans la base (e_1, e_2, e_3, e_4) est $I_2 \otimes A$. On a donc $\det(A \otimes I_2) = \det u = (\det A)^2$ d'après ce qui précède. D'après la première question, $A \otimes B = (A \otimes I_2) \cdot (I_2 \otimes B)$. Ainsi $\det(A \otimes B) = \det(A)^2 \det(B)^2$.
3. Puisqu'une matrice est inversible si et seulement si son déterminant est non nul, d'après la question précédente, $A \times B$ est inversible si et seulement si A et B le sont. Dans ce cas, on a d'après la première question
$$(A \otimes B) \cdot (A^{-1} \otimes B^{-1}) = (AA^{-1}) \otimes (BB^{-1}) = I_2 \otimes I_2 = I_4$$

4. D'après l'énoncé, il existe $P, Q \in Gl_n(\mathbb{K})$ et $D_A, D_B \in \mathcal{M}_n(\mathbb{K})$ diagonales tels que : $A = PD_AP^{-1}$ et $B = QD_BQ^{-1}$.
On montre aisément que :

$$(A \otimes B) = (P \otimes Q)(D_A \otimes D_B)(P^{-1} \otimes Q^{-1})$$

Ce qui justifie que $(A \otimes B)$ est diagonalisable.

XIII.2.5 Disques de Gershgorin

[Enoncé]

XIII.2.6 Spectre de $u \circ v$ et $v \circ u$

[Enoncé]

XIII.2.7 Endomorphismes qui commutent

[Enoncé]

XIII.2.8 Vecteur propre commun

[Enoncé]

XIII.2.9 Eléments propres d'un endomorphisme (1)

[Enoncé]

XIII.2.10 Eléments propres d'un endomorphisme (2)

[Enoncé]

XIII.2.11 Eléments propres d'un endomorphisme (3)

[Enoncé]

XIII.2.12 Eléments propres d'un endomorphisme (4)

[Enoncé]

XIII.2.13 Loi de Hooke

[Enoncé]

XIII.2.14 Existence d'une valeur propre double

[Enoncé]

XIII.2.15 Détermination de spectre

[Enoncé]

XIII.2.16 Sommes et produits de valeurs propres

[Enoncé]

XIII.2.17 Matrice compagnon (1)

[Enoncé]
Vous pouvez espérer que dire : "On développe par rapport à la dernière colonne pour en déduire le résultat" sans justifier les calculs suffira à convaincre le correcteur, mais il y a de fortes chances qu'il n'apprécie pas.
On va donc montrer de façon rigoureuse que :

$$C_P = P$$

Pour visualiser un peu, écrivons le polynôme caractéristique sous forme de déterminant :

$$C_P(X) = \begin{vmatrix} X & 0 & \dots & \dots & \dots & 0 & a_0 \\ -1 & X & 0 & \dots & \dots & 0 & a_1 \\ 0 & \ddots & \ddots & \ddots & & \vdots & a_2 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & 0 & \vdots \\ \vdots & & & \ddots & \ddots & X & a_{n-2} \\ 0 & \dots & \dots & \dots & 0 & -1 & X - a_{n-1} \end{vmatrix}$$

On procède aux opérations suivantes :

$$L_1 \leftarrow L_1 + X^i L_i$$

Ainsi, on a :

$$C_P(X) = \begin{vmatrix} 0 & 0 & \dots & \dots & \dots & 0 & P(X) \\ -1 & X & 0 & \dots & \dots & 0 & a_1 \\ 0 & \ddots & \ddots & \ddots & & \vdots & a_2 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & 0 & \vdots \\ \vdots & & & \ddots & \ddots & X & a_{n-2} \\ 0 & \dots & \dots & \dots & 0 & -1 & X - a_{n-1} \end{vmatrix}$$

En développant par rapport à la première ligne, on a :

$$C_P(X) = P(X)(-1)^{n+1} \begin{vmatrix} -1 & X & 0 & \dots & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & 0 \\ \vdots & & & \ddots & \ddots & X \\ 0 & \dots & \dots & \dots & 0 & -1 \end{vmatrix}$$

Ainsi, on a montré que $C_P = P$.

XIII.2.18 Réduction de la transposée d'une matrice

[Enoncé]

1. On sait que pour tout $M \in \mathcal{M}_n(\mathbb{K}), \det(M) = \det(M^\top)$.
   Ainsi,
   $$\chi_A = \det(XI_n - A) = \det((XI_n - A)^\top) = \det(XI_n - A^\top) = \chi_{A^\top}$$

2. On sait que pour tout $M \in \mathcal{M}_n(\mathbb{K}), \mathrm{rg}(M) = \mathrm{rg}(M^\top)$.
   Ainsi, d'après le théorème du rang :
   $$\dim(E_\lambda(A)) = \dim(\mathrm{Ker}(A - \lambda I_n)) = \dim(\mathrm{Ker}(A^\top - \lambda I_n)) = \dim(E_\lambda I_n)$$

3. Supposons que A est diagonalisable. Alors
   $$n = \sum_{\lambda \in \mathrm{Sp}(A)} \dim(E_\lambda(A))$$

.
Ainsi, à l'aide de la question précédente, on montre aisément que

$$n = \sum_{\lambda \in \mathrm{Sp}(A^\top)} \dim(E_\lambda(A^\top))$$

.
Donc $A^\top$ est diagonalisable.
Puisque $(A^\top)^\top = A$, la réciproque est immédiate.

XIII.2.19 Algorithme de Faddeev

[Enoncé]

XIII.2.20 Endomorphisme de transposition

[Enoncé]
On prend la base canonique $(E_{i,j})$ de $\mathcal{M}_n(\mathbb{R})$.
On remarque que :

$$\forall (i,j) \in (\llbracket 1; n \rrbracket)^2, \Phi(E_{i,j}) = E_{j,i}$$

Ainsi,

- les matrices $E_{i,i}$ sont les vecteurs propres de Φ,
- pour chaque paire (i,j) avec $i < j$, l'espace engendré par $E_{i,j}, E_{j,i}$ est stable par Φ. Dans cette base, Φ a pour matrice

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

dont les valeurs propres sont -1 et 1.

Par conséquent, puisque $\det(\Phi) = \prod_{\lambda \in \mathrm{Sp}(\Phi)} \lambda$ et $\mathrm{Tr}(\Phi) = \sum_{\lambda \in \mathrm{Sp}(\Phi)} \lambda$, on a :

$$\det(\Phi) = (-1)^{\frac{n(n-1)}{2}} \text{ et } \mathrm{Tr}(\Phi) = \frac{n(n+1)}{2} + \frac{n(n-1)}{2} = n$$

XIII.2.21 Exemple de matrice non diagonalisable

[Enoncé]

1. La matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ n'est pas diagonalisable sur $\mathbb{C}$.
2. La matrice $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ est diagonalisable sur $\mathbb{C}$ mais pas sur $\mathbb{R}$.

3. On pose $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.
   Ces deux matrices sont diagonalisables et pourtant :
$$A + B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$
   n'est pas diagonalisable.
4. $$AB = \begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix}$$
   n'est pas diagonalisable.

XIII.2.22 Diagonalisabilité d'une matrice (1)

[Enoncé]

XIII.2.23 Diagonalisabilité d'une matrice (2)

[Enoncé]

XIII.2.24 Diagonalisibilité d'une matrice (3)

[Enoncé]

XIII.2.25 Cotrigonalisation (1)

[Enoncé]

XIII.2.26 Cotrigonalisation (2)

[Enoncé]

XIII.2.27 Cotrigonalisation (3)

[Enoncé]

XIII.2.28 Cotrigonalisation (4)

[Enoncé]

XIII.2.29 Cotrigonalisation (5)

[Enoncé]

XIII.2.30 Caractérisation des matrices nilpotente par la trace

[Enoncé]

XIII.2.31 Facteur commun dans le polynôme caractéristique

[Enoncé]

XIII.2.32 $\chi_{AB} = \chi_{BA}$

[Enoncé

XIII.2.33 Polynôme caractéristique de l'inverse

[Enoncé]

XIII.2.34 Commutativité et stabilité

[Enoncé]

XIII.2.35 Dimension du commutant d'une matrice diagonalisable

[Enoncé]

XIII.2.36 Sous-espaces stables d'un endomorphisme diagonalisable

[Enoncé]

XIII.2.37 Hyperplans stables

[Enoncé]

XIII.2.38 Endomorphisme qui stabilise un nombre fini de sous-espaces ★★★

[Enoncé]
On pose $\mathrm{Sp}(u) = \{\lambda_1, \dots, \lambda_n\}$.
Et on note $E_1, \dots, E_n$ les sous-espaces propres de u respectivement associés à $\lambda_1, \dots, \lambda_n$.
On remarque que pour toute partie I de $[\![1; n]\!]$, $\bigoplus_{i\in I} E_i$ est stable par u.
Ainsi, il existe au moins 2^n sous-espaces vectoriels stables par u. D'après l'exercice XIII.2.36, pour tout sous-espace vectoriel F stable par u, on a : $F = \bigoplus_{i=1}^{n} F \cap E_i$. Or pour tout $i \in [\![1; n]\!]$, $F \cap E_i$ est un sous-espace vectoriel de E_i.
Donc puisque $\dim(E_i) = 1$, on a $F \cap E_i = \{0\}$ ou $F \cap E_i = E_i$ pour tout $i \in [\![1; n]\!]$.
Par conséquent, F est une somme de sous-espaces propres.
Ainsi, les seuls espaces vectoriels stables par u sont de la forme $\bigoplus_{i\in I} E_i$ avec I une partie de $[\![1; n]\!]$. Il y a donc 2^n espaces vectoriels stables par u.

XIII.2.39 Sous-espaces stables d'un endomorphisme nilpotent maximal ★★★

[Enoncé]
On montre classiquement qu'il existe $x \in E$ tel que $(x, u(x), \dots, u^{n-1}(x))$ est une base de E.
On remarque que $\{0\} \subset \ker(u) \subset \cdots \subset \ker(u^{n-1}) \subset E$.
Montrons que : $\forall p \in [\![1; n]\!], \dim(\ker(u^p)) = p$. Puisque $\mathcal{B} = (x, u(x), \dots, u^{n-1}(x))$ est une base de E, la matrice de u dans cette base est :

$$\mathrm{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 \\ 1 & \ddots & \ddots & & \vdots \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

Donc en calculant les puissances de cette matrice :

$$\mathrm{Mat}(u^p) = \mathrm{Mat}_{\mathcal{B}}(u)^p = \begin{pmatrix} 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots & \vdots & & \vdots \\ 0 & \cdots & \cdots & 0 & \vdots & & \vdots \\ 1 & 0 & \cdots & 0 & \vdots & & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & & \vdots \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{pmatrix}$$

on en déduit que la dimension de $\ker(u^p)$ est égale à p pour tout $p \in [\![1; n-1]\!]$.
Soit F un espace stable par u de dimension $p \in [\![1; n-1]\!]$.
En étudiant l'endomorphisme induit u_F par u sur F, on a que u_F est nilpotent puisque $u_F^n = 0$ et donc $u_F^p = 0$ puisque $u_F \in \mathcal{L}(F)$.
Donc $F \subset \ker(u^p)$.
Et donc avec $\dim(F) = \dim(\ker(u^p))$, on a $F = \ker(u^p)$.
Finalement, les espaces vectoriels stables par u sont les $\ker(u^p)$ pour tout $p \in [\![0; n]\!]$ ce qui donne bien qu'il y a exactement $n+1$ espaces vectoriels stables par u.

XIII.2.40 Sous-espaces stables par tous les endomorphismes de permutation ★★★★

[Enoncé]

1. Notons $\mathcal{B} = (e_1, \ldots, e_n)$ la base canonique de $\mathbb{C}^n$. On note aussi $\sigma = \sigma_1 \circ \cdots \circ \sigma_r$ la décomposition en cycles à supports disjoints de σ ainsi que l_i la longueur de σ_i pour $i \in [\![1; r]\!]$.
   On remarque que $\forall \tau, \tau' \in \mathcal{S}_n,\ u_{\tau\circ\tau'} = u_{\tau'} \circ u_\tau$ et que u_τ laisse laisse invariant e_i lorsque i n'est pas dans son support. Ainsi il suffit de déterminer la matrice de $u_{\sigma_1}, \ldots, u_{\sigma_r}$ pour avoir celle de u_σ.
   Traitons d'abord le cas simple : $\sigma = (1, \ldots, n)$. Dans ce cas, la matrice de u_σ dans la base $\mathcal{B}$ est

$$P_n := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

   On remarque que P_n est une matrice compagnon (cf. II.17) donc $\chi_{u_\sigma} = X^n - 1$.
   Ensuite, pour un cycle quelconque $\sigma = (i_1, \ldots, i_p)$ de $\mathcal{S}_n$, de manière similaire la matrice

de u_σ dans la base $\mathcal{B}' = (e_{j_1}, \dots, e_{j_{n-p}}, e_{i_1}, \dots, e_{i_p})$ avec $j_1, \dots, j_{n-p}$ les points fixes de σ est :

$$M = \left(\begin{array}{c|c} I_{n-p} & 0 \\ \hline 0 & P_p \end{array}\right)$$

Où $P_p \in \mathcal{M}_p(\mathbb{C})$ est de la même forme que P_n. Donc $\chi_{u_\sigma} = (X-1)^{n-p}(X^p-1)$.
Enfin, dans le cas général on note $j_1, \dots, j_k$ les points fixes de σ ainsi que $\sigma_m = (i_{m,1}, \dots, i_{m,l_m})$ pour $i \in [\![1;r]\!]$. Si $s \in [\![1;n]\!]$ est dans le support de σ alors il est dans un, et seulement un des supports de $\sigma_1, \dots, \sigma_r$. Disons que $s = i_{m,t}$. Donc $u_\sigma(e_s) = u_{\sigma_m}(e_{i_{m,t}}) = \begin{cases} e_{i_{m,t+1}} & \text{si } t < l_m \\ e_{i_{m,1}} & \text{si } t = l_m \end{cases}$.
Autrement dit, la matrice de u_σ dans la base B', concaténation des bases $B_0 = (e_{j_1}, \dots, e_{j_k})$ et $B_m = (e_{i_{m,1}}, \dots, e_{i_{m,l_m}})$ pour $1 \leq m \leq r$ est :

$$M = \left(\begin{array}{c|c|c|c|c} I_k & 0 & \cdots & \cdots & 0 \\ \hline 0 & P_{l_1} & 0 & \cdots & 0 \\ \hline \vdots & 0 & \ddots & \ddots & \vdots \\ \hline \vdots & \vdots & \ddots & \ddots & \vdots \\ \hline 0 & 0 & \cdots & 0 & P_{l_r} \end{array}\right)$$

Par conséquent $\chi_{u_\sigma} = (X-1)^k \prod_{i=1}^{r} (X^{l_i}-1)$ et $\mathrm{Sp}(u_\sigma) = \bigcup_{i=1}^{r} \mathbb{U}_{l_i}$.

Remarque : Vu la forme de la matrice de u_σ, on peut montrer que $\pi_{u_\sigma} = \mathrm{ppcm}(X^{l_1}-1, \dots, X^{l_r}-1) = X^{\mathrm{ppcm}(l_1,\dots,l_r)}-1$.

2. On note encore $(e_1, \dots, e_n)$ la base canonique de $\mathbb{C}^n$ et on note pour $(i,j) \in [\![1;n]\!]^2$ avec $i \neq j$, $\tau_{i,j}$ la transposition (i,j). Pour comprendre l'idée du raisonnement on va d'abord traiter le cas $n = 3$.
Soit V un sev non nul de $\mathbb{C}^3$ stables par tous les u_σ, $\sigma \in \mathcal{S}_3$.
Fixons $x = (x_1, x_2, x_3) \in V$. On sait que $u_{\tau_{1,2}}(x) = x_2 e_1 + x_1 e_2 + x_3 e_3 \in V$. Il est alors naturel de considérer la différence $u_{\tau_{1,2}}(x) - x = (x_2 - x_1)e_1 + (x_1 - x_2)e_2 = (x_2 - x_1)(e_1 - e_2) \in V$. Si $x_2 - x_1 \neq 0$ cela donne $e_1 - e_2 \in V$. Mais en considérant $u_{\tau_{1,2}\circ\tau_{2,3}}(x) = u_{\tau_{2,3}}(u_{\tau_{1,2}}(x)) = x_2 e_1 + x_3 e_2 + x_1 e_3$ on obtient de la manière que $e_1 - e_3 \in V$. Alors pour des raisons de dimensions $V = \mathrm{Vect}(e_1 - e_2, e_1 - e_3)$ ou $V = \mathbb{C}^3$.
De plus le raisonnement s'adapte tant qu'il existe un vecteur $x \in V$ dont deux composantes au moins diffèrent. C'est cela que l'on va chercher à généraliser.
Soit V un sev non nul de $\mathbb{C}^n$ stables par tous les u_σ pour $\sigma \in \mathcal{S}_n$. Supposons qu'il existe un vecteur $x = (x_1, \dots, x_n) \in V$ dont deux composantes au moins diffèrent. On note $i < j$ tel que $x_i \neq x_j$.
On pose pour $k \neq j$, $y_k = u_{\tau_{k,j}}(x) \in V$. En notant $y_k = (y_{k,1}, \dots, y_{k,n})$ on sait que $y_{k,i} = x_i \neq x_j = y_{k,k}$. On sait alors que $u_{\tau_{i,k}}(y) - y = (x_j - x_i)(e_i - e_k) \in V$ ce qui impose $e_i - e_k \in V$. Ceci étant vrai pour tout $k \neq i$, V contient l'hyperplan

$H = \text{Vect}(e_i - e_k,\ k \neq i)$. Donc V est soit de dimension $n-1$ et égal à H, soit de dimension n et égal à $\mathbb{C}^n$.

Réciproquement on vérifie aisément que $\{0\}, \text{Vect}((1,\dots,1)), H = \left\{(x_1,\dots,x_n) \in \mathbb{C}^n,\ \sum_{i=1}^{n} x_i = 0\right\}$ et $\mathbb{C}^n$ sont stables par tous les $u_\sigma,\ \sigma \in \mathfrak{S}_n$.

XIII.2.41 Semi-simplicité

[Enoncé]

XIII.2.42 Endomorphismes diagonalisables d'un $\mathbb{R}$-espace vectoriel

[Enoncé]

XIII.2.43 Matrices à spectres disjoints

[Enoncé]

• (i)$\Longrightarrow$(ii) :

Pour tout $\lambda \in \text{Sp}(A)$, on a $B - \lambda I_n \in \text{GL}_n(\mathbb{K})$ car $\lambda \not\in \text{Sp}(B)$.

Ainsi par produit, $\chi_A(B)$ est inversible.

• (ii)$\Longrightarrow$ (iii) :

Soit $X \in \mathcal{M}_n(\mathbb{K})$ tel que $AX = XB$.

On montre par récurrence que

$$\forall k \in \mathbb{N}, A^k X = XB^k$$

Ainsi pour tout $P \in \mathbb{K}[X]$,

$$P(A)X = XP(B)$$

En particulier, pour $P = \chi_A$, on a d'après Cayley-Hamilton :

$$0 = \chi_A(A)X = X\chi_A(B)$$

Et puisque que $\chi_A(B)$ est inversible, on en déduit que $X = 0$.

• (iii)$\Longrightarrow$ (iv) :

On pose l'application

$$\varphi : \left\{ \begin{array}{ccc} \mathcal{M}_n(K) & \longrightarrow & \mathcal{M}_n(\mathbb{K}) \\ X & \longmapsto & AX - XB \end{array} \right.$$

On montre aisément que φ est linéaire. Et puisque $\mathcal{M}_n(\mathbb{K})$ est de dimension finie et que l'on a supposé que φ est injectif. On en déduit que φ est bijectif.

En particulier, φ est surjective d'où le résultat.

• (iv)$\Longrightarrow$(i) :

Raisonnons par l'absurde que A et B possède une valeur propre commune λ.

Soit $u, v \in \mathcal{M}_{n,1}(\mathbb{K})$ tel que u est un vecteur propre de $A^\top$ et v est un vecteur propre de B pour la valeur propre λ. Ainsi pour tout $X \in \mathcal{M}_n(\mathbb{K})$,

$$u^\top AXv - u^\top XBv = 0$$

Ainsi, il suffit de trouver une matrice M tel que$u^\top Mv$ est non nulle. On peut prendre $M = uv^\top$.
Ainsi, on obtient une contradiction, donc A et B sont à spectres disjoints.

XIII.3 Correction Réduction algébrique

XIII.3.1 Equation matricielle polynomiale (1)

[Enoncé]
On raisonne par analyse synthèse. Soit $M \in \mathcal{M}_n(\mathbb{C})$ telle que $M^5 = M^2$ et $\mathrm{Tr}(M) = n$.
Le polynôme $X^5 - X^2 = X^2(X^3 - 1)$ annule M donc $\mathrm{Sp}(M) \subset \{0, 1, j, \overline{j}\}$ en notant $j = e^{2i\pi/3}$.
On note m_λ la multiplicité de $\lambda \in \mathbb{C}$ en tant que valeur propre de M ($m_\lambda = 0$ si λ n'est pas valeur propre de M).
$\mathrm{Tr}(M) = n \iff jm_j + \overline{j}m_{\overline{j}} + m_1 = n$. En comparant la partie réelle et la partie imaginaire on obtient $\begin{cases} m_1 - \dfrac{m_j + m_{\overline{j}}}{2} = n \\ \dfrac{\sqrt{3}}{2}(m_j - m_{\overline{j}}) = 0 \end{cases}$ Donc $m_j = m_{\overline{j}}$ et par suite $m_1 - m_j = n$.
Or $\forall \lambda \in \mathbb{C},\ m_\lambda \in [\![0; n]\!]$ et de plus $m_0 + m_1 + m_j + m_{\overline{j}} = n$. Donc $m_1 = n$ et $m_j = m_{\overline{j}} = m_0 = 0$. Autrement dit 1 est la seule valeur propre de M. Mais alors en particulier M est inversible d'où $M^3 = I_n$.
Le polynôme $X^3 - 1$ annule M donc M est diagonalisable. N'ayant que 1 pour valeur propre, on conclut que $M = I_n$.
Enfin I_n vérifie évidemment $I_n^5 = I_n^2$.

XIII.3.2 Equation matricielle polynomiale (2)

[Enoncé]
Soit $A \in \mathcal{M}_n(\mathbb{R})$ telle que $A^3 + A^2 + A = 0$. Le polynôme $X^3 + X^2 + X = X(X^2 + X + 1)$ annule A donc $\mathrm{Sp}(A) \subset \{0, j, \overline{j}\}$ en notant $j = e^{2i\pi/3}$.
Pour $\lambda \in \mathbb{C}$ on note m_λ la multiplicité de λ en tant que valeur propre de A, càd en tant que racine de son polynôme caractéristique ($m_\lambda = 0$ si λ n'est pas valeur propre de A).
Comme A est à coefficients réels, $\chi_A \in \mathbb{R}[X]$. Donc $m_j = m_{\overline{j}}$. De plus d'après le théorème du rang $\mathrm{rg}(A) = n - m_0$.
Enfin on sait que $m_0 + m_j + m_{\overline{j}} = n$ càd $2m_j = n - m_0 = \mathrm{rg}(A)$. $\mathrm{rg}(A)$ est donc pair.

XIII.3.3 Equation matricielle avec la comatrice

[Enoncé]

1. On sait que si $M \in \mathrm{GL}_n(\mathbb{C})$ on a $\mathrm{Com}(M)^\top = \det(M)M^{-1}$.
   Soit $A, B \in \mathrm{GL}_n(\mathbb{C})$. $\det(AB) = \det(A)\det(B) \neq 0$ donc $AB \in \mathrm{GL}_n(\mathbb{C})$.
   Ainsi $\mathrm{Com}(AB)^\top = \det(AB)(AB)^{-1} = \det(B)B^{-1}\det(A)A^{-1} = \mathrm{Com}(B)^\top \mathrm{Com}(A)^\top$ i.e $\mathrm{Com}(AB) = \mathrm{Com}(A)\mathrm{Com}(B)$.
   Soit maintenant $A, B \in \mathcal{M}_n(\mathbb{C})$. On sait que $\mathrm{GL}_n(\mathbb{C})$ est dense dans $\mathcal{M}_n(\mathbb{C})$ cf.[l'exo qui va bien] donc il existe deux suites de matrices inversibles $(A_k)_{k\in\mathbb{N}}$ et $(B_k)_{k\in\mathbb{N}}$ de limites respectives A et B.

D'après ce qui vient d'être fait, $\forall k \in \mathbb{N},\ \mathrm{Com}(A_kB_k) = \mathrm{Com}(A_k)\,\mathrm{Com}(B_k)$.
Or les coefficients de $\mathrm{Com}(M)$ sont polynomiaux en ceux de M, donc l'application $\mathrm{Com} : M \in \mathcal{M}_n(\mathbb{C}) \mapsto \mathrm{Com}(M)$ est continue. D'autre part le produit matriciel $(M,N) \in \mathcal{M}_n(\mathbb{C})^2 \mapsto MN$ est bilinéaire sur $\mathcal{M}_n(\mathbb{C})$ qui est un espace vectoriel de dimension $n^2 < \infty$. C'est donc aussi une application continue.
On en déduit par passage à la limite que $\mathrm{Com}(AB) = \mathrm{Com}(A)\,\mathrm{Com}(B)$.

2. Soit $\lambda \in \mathbb{C}$ et soit $A \in E_\lambda$. Soit enfin $P \in \mathrm{GL}_n(\mathbb{C})$. On pose $B = PAP^{-1}$.
D'après la question précédente $\mathrm{Com}(B) = \mathrm{Com}(P)\,\mathrm{Com}(A)\,\mathrm{Com}(P^{-1})$.
Or toujours d'après la question précédente $I_n = \mathrm{Com}(I_n) = \mathrm{Com}(PP^{-1}) = \mathrm{Com}(P)\,\mathrm{Com}(P^{-1})$.
Donc $\mathrm{Com}(P^{-1}) = \mathrm{Com}(P)^{-1}$. Et comme P est inversible, $\mathrm{Com}(P)^\top = \det(P)P^{-1}$.
Ainsi, $\mathrm{Com}(B)^\top = P\,\mathrm{Com}(A)^\top P^{-1}$ et par suite $B+\mathrm{Com}(B)^\top = P(A+\mathrm{Com}(A)^\top)P^{-1} = \lambda I_n$.
C'est-à-dire $B \in E_\lambda$.

3. On note $\tilde{A} = \mathrm{Com}(A)^\top$. $\mathrm{rg}(\tilde{A}) = \mathrm{rg}(\mathrm{Com}(A))$.
Pour $n = 1$ on déduit de la formule $A\tilde{A} = \det(A)I_n$ que $\tilde{A} = 1$ si $A \neq 0$. $\tilde{A} = 0$ si $A = 0$. On suppose donc maintenant $n \geq 2$.
Si $\mathrm{rg}(A) = n$ i.e si A est inversible, alors $\tilde{A}$ est inversible puisque $A\tilde{A} = \det(A)I_n$ avec $\det(A) \neq 0$.
Si $\mathrm{rg}(A) \leq n-2$ alors tous les mineurs de A sont nuls, comme déterminants de matrices extraites de A de tailles strictement supérieures à $\mathrm{rg}(A)$ donc $\tilde{A} = 0$ i.e $\mathrm{rg}(\tilde{A}) = 0$.
Enfin, supposons que $\mathrm{rg}(A) = n-1$. On a $A\tilde{A} = \det(A)I_n = 0$. Donc $\mathrm{Im}(\tilde{A}) \subset \mathrm{Ker}(A)$.
D'après le théorème du rang $\mathrm{Ker}(A)$ est de dimension 1, donc $\tilde{A}$ est de rang 1 ou 0.
$\mathrm{Com}(A)$ n'est pas nulle puisque A, de rang $n-1$, a au moins un mineur non nul. On en déduit que $\mathrm{rg}(\tilde{A}) = 1$.
En résumé, $\mathrm{rg}(\mathrm{Com}(A)) = \begin{cases} n & \text{si } \mathrm{rg}(A) = n \\ 1 & \text{si } 0 < \mathrm{rg}(A) = n-1 \\ 0 & \text{sinon} \end{cases}$

4. On note toujours $\tilde{A} = \mathrm{Com}(A)^\top$.
Pour $n = 1$, toute matrice A appartient à $E_{A+\tilde{A}}$. Supposons dans la suite $n \geq 2$.
Soient $\lambda \in \mathbb{C}$ et $A \in \mathcal{M}_n(\mathbb{C})$ tels que $A+\tilde{A} = \lambda I_n$. Observons qu'en multipliant l'égalité par A il vient $A^2 - \lambda A - \det(A)I_n = 0$. On va discuter selon le rang de A.
Si $\mathrm{rg}(A) \leq n-2$ alors $\tilde{A} = 0$ et par suite $A = \lambda I_n$. Comme A n'est pas inversible on a $\lambda = 0$ d'où $A = 0$. La matrice nulle est bien dans E_0.
Supposons que $\mathrm{rg}(A) = n-1$.
Supposons dans un premier temps que $\lambda \neq 0$. Alors $A(A-\lambda I_n) = 0$ et le polynôme $X(X-\lambda)$ est scindé à racines simples. Donc A est diagonalisable et puisque $\mathrm{rg}(A) = n-1$, A est semblable à la matrice $\lambda J_{n-1} = \mathrm{diag}(\lambda,\dots,\lambda,0)$. On calcule $\mathrm{Com}(\lambda J_{n-1}) = \left(\begin{array}{ccc|c} & & & 0 \\ & 0 & & \vdots \\ & & & 0 \\ \hline 0 & \cdots & 0 & \lambda^{n-1} \end{array}\right)$. La matrice A appartient donc à E_λ ssi

$\lambda^{n-1} = \lambda$, autrement dit ssi λ est une racine $(n-2)$-ième de l'unité.
Maintenant si $\lambda = 0$ alors $A^2 = 0$. Ceci impose $\mathrm{Im}(A) \subset \mathrm{Ker}(A)$ et par le théorème du rang $n - 1 = \mathrm{rg}(A) \leq \dim \mathrm{Ker}(A) = 1$ i.e $n \leq 2$. Donc E_0 est vide lorsque $n > 2$.
Pour le cas $n = 2$, on écrit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. On calcule $\mathrm{Com}(A) = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$ puis $A + \tilde{A} = \begin{pmatrix} a+d & 0 \\ 0 & a+d \end{pmatrix} = \mathrm{Tr}(A) I_n$. Ainsi $\forall A \in \mathcal{M}_2(\mathbb{C}),\ A \in E_{\mathrm{Tr}(A)}$.
On s'intéressera dans la suite au cas $n \geq 3$.
Supposons enfin $\mathrm{rg}(A) = n$. On note Δ le discriminant de $P(X) = X^2 - \lambda X - \det(A)$. Si $\Delta \neq 0$ alors P est scindé à racines simples donc A est diagonalisable. On note λ_1, λ_2 les deux racines de P et m la multiplicité de λ_1 en tant que valeur propre de A. On peut remarquer qu'avec ses notations, $\lambda = \lambda_1 + \lambda_2$ et $\det(A) = \lambda_1 \lambda_2$.
A est semblable à la matrice diagonale $D = \mathrm{diag}(\lambda_1, \dots, \lambda_1, \lambda_2, \dots, \lambda_2)$ où λ_1 apparaît m fois et λ_2 apparaît $n - m$ fois.
Alors $\lambda_1 \lambda_2 = \det(A) = \det(D) = \lambda_1^m \lambda_2^{n-m}$. Comme A est inversible $\lambda_1 \neq 0$ et $\lambda_2 \neq 0$. Ainsi λ_1, λ_2 vérifient la relation $\lambda_1^{m-1} = \lambda_2^{m+1-n}$.
Etudions la réciproque. Si $D = \mathrm{diag}(\lambda_1, \dots, \lambda_1, \lambda_2, \dots, \lambda_2) \in \mathrm{GL}_n(\mathbb{C})$, où λ_1 apparaît $m \in [\![1; n-1]\!]$ fois et $\lambda_1^{m-1} = \lambda_2^{m+1-n}$ alors on calcule $\tilde{D} = \det(D) D^{-1} = \lambda_1 \lambda_2 \,\mathrm{diag}(\lambda_1^{-1}, \dots, \lambda_1^{-1}, \lambda_2^{-1}, \dots, \lambda_2^{-1}) = \mathrm{diag}(\lambda_2, \dots, \lambda_2, \lambda_1, \dots, \lambda_1)$ où λ_2 apparaît m fois.
Donc $D + \tilde{D} = (\lambda_1 + \lambda_2) I_n$.
Reste à traiter le cas $\Delta = 0$ càd $\lambda^2 = 4 \det(A)$. On note $\mu = \dfrac{\lambda}{2} \neq 0$ la racine double de P. On a $\det(A) = \mu^n = \mu_2$ donc μ est une racine $(n-2)$-ième de l'unité.
réciproquement fixons $\mu \in \mathbb{U}_{n-2}$ et $A \in \mathcal{M}_n(\mathbb{C})$ telle que $B = A - \mu I_n$ vérifie $B^2 = 0$. Alors μ est l'unique valeur propre de A et $\det(A) = \mu^n = \mu^2$. $B^2 = 0 \implies A^2 - 2\mu A + \mu^2 I_n = 0 \implies -\dfrac{1}{\mu^2} A^2 + \dfrac{2}{\mu} A = I_n \implies A^{-1} = \dfrac{2}{\mu} I_n - \dfrac{1}{\mu^2} A$. On calcule alors $A + \tilde{A} = A + \det(A) A^{-1} = A + \mu^2 \left(\dfrac{2}{\mu} I_n - \dfrac{1}{\mu^2} A \right) = 2\mu I_n$.

En outre on peut résumer la réponse en :

- $\forall A \in \mathcal{M}_1(\mathbb{C}),\ A \in E_{A+\tilde{A}}$;
- $\forall A \in \mathcal{M}_2(\mathbb{C}),\ A \in E_{\mathrm{Tr}(A)}$;
- Si $n \geq 3$ et si $A \in E_\lambda$ alors,
  - si $\mathrm{rg}(A) < n - 2$ alors $\lambda = 0$ et $A = 0$;
  - si $\mathrm{rg}(A) = n - 1$ alors $\lambda \in \mathbb{U}_{n-2}$ et $A \sim \lambda J_{n-1} = \mathrm{diag}(\lambda, \dots, \lambda, 0)$;
  - si $\mathrm{rg}(A) = n$ alors,
    - si $\lambda^2 \neq 4 \det(A)$ alors A a deux valeurs propres distinctes λ_1 et λ_2, $\lambda = \lambda_1 + \lambda_2$ et A est semblable à une matrice de la forme $\mathrm{diag}(\lambda_1, \dots, \lambda_1, \lambda_2, \dots, \lambda_2)$ où λ_1 apparaît $m \in [\![1; n-1]\!]$ fois. De plus λ_1, λ_2 vérifient la relation $\lambda_1^{m-1} = \lambda_2^{m+1-n}$;

— si $\lambda^2 = 4\det(A)$ alors $\dfrac{\lambda}{2} \in \mathbb{U}_{n-2}$ et $\left(A - \dfrac{\lambda}{2} I_n\right)^2 = 0$.

XIII.3.4 Rang et spectre de la comatrice

Pour $n = 1$ on déduit de la formule $A\tilde{A} = \det(A) I_n$ que $\tilde{A} = 1$ si $A \neq 0$. $\tilde{A} = 0$ si $A = 0$.
On suppose donc maintenant $n \geq 2$.
Si $\mathrm{rg}(A) = n$ i.e si A est inversible, alors $\tilde{A}$ est inversible puisque $A\tilde{A} = \det(A) I_n$ avec $\det(A) \neq 0$.
Si $\mathrm{rg}(A) \leq n-2$ alors tous les mineurs de A sont nuls, comme déterminants de matrices extraites de A de tailles strictement supérieures à $\mathrm{rg}(A)$ donc $\tilde{A} = 0$ i.e $\mathrm{rg}(\tilde{A}) = 0$.
Enfin, supposons que $\mathrm{rg}(A) = n-1$. On a $A\tilde{A} = \det(A) I_n = 0$. Donc $\mathrm{Im}(\tilde{A}) \subset \mathrm{Ker}(A)$. D'après le théorème du rang $\mathrm{Ker}(A)$ est de dimension 1, donc $\tilde{A}$ est de rang 1 ou 0. $\tilde{A}$ n'est pas nulle puisque A, de rang $n-1$, a au moins un mineur non nul. On en déduit que $\mathrm{rg}(\tilde{A}) = 1$.

En résumé, $\mathrm{rg}(\tilde{A}) = \begin{cases} n & \text{si } \mathrm{rg}(A) = n \\ 1 & \text{si } 0 < \mathrm{rg}(A) = n-1 \\ 0 & \text{sinon} \end{cases}$

Pour ce qui est du spectre, l'étude du rang nous permet déjà de dire que $\mathrm{Sp}(\tilde{A}) = \{0\}$ si $\mathrm{rg}(A) < n-1$. Si $\mathrm{rg}(A) = n-1$ alors $\tilde{A}$ est de rang 1. On en déduit qu'il existe $\lambda \in \mathbb{C}$ tel que $\chi_{\tilde{A}}(X) = X^{n-1}(X - \lambda)$. Comme on sait que le coefficient en X^{n-1} de $\chi_{\tilde{A}}$ est $-\mathrm{Tr}(\tilde{A})$ on en déduit que $\lambda = \mathrm{Tr}(\tilde{A})$. Donc $\mathrm{Sp}(\tilde{A}) = \{0, \mathrm{Tr}(\tilde{A})\}$ (On a potentiellement $\mathrm{Tr}(\tilde{A}) = 0$).
Enfin supposons que $\tilde{A}$ est inversible. Fixons $\lambda \in \mathbb{C}^*$.

$$\begin{aligned}
\chi_{\tilde{A}}(\lambda) &= \det(\lambda I_n - \tilde{A}) \\
&= \det(A^{-1}) \det(\lambda A - A\tilde{A}) \\
&= \frac{1}{\det(A)} \det(\lambda A - \det(A) I_n) \\
&= \frac{(-\lambda)^n}{\det(A)} \det\left(\frac{\det(A)}{\lambda} I_n - A\right) \\
&= \frac{\lambda^n}{(-1)^n \det(A)} \chi_A\left(\frac{\det(A)}{\lambda}\right)
\end{aligned}$$

$\mathbb{C}^*$ étant infini on a l'égalité entre polynômes $\chi_{\tilde{A}}(X) = \dfrac{X^n}{(-1)^n \det(A)} \chi_A\left(\dfrac{\det(A)}{X}\right)$.
On sait que $\tilde{A}$ est inversible donc $\lambda = 0$ n'est pas racine de $\chi_{\tilde{A}}$.
Ainsi $\forall \lambda \in \mathbb{C},\ \chi_{\tilde{A}}(\lambda) = 0 \iff \chi_A\left(\dfrac{\det(A)}{\lambda}\right) = 0 \iff \dfrac{\det(A)}{\lambda} \in \mathrm{Sp}(A)$.
Finalement $\mathrm{Sp}(\tilde{A}) = \{\det(A)\mu^{-1},\ \mu \in \mathrm{Sp}(A)\}$.

XIII.3.5 Racine p-ième d'une matrice

[Enoncé]

$\mathcal{M}_{n,1}(\mathbb{C}) = \bigoplus_{\lambda\in \mathrm{Sp}(B^p)} \ker(B^p - \lambda \mathrm{Id})$.
Posons pour $\lambda \in \mathrm{Sp}(A)$ et $k \in [\![0; p-1]\!]$, $\mu_{\lambda,k} = \sqrt[p]{|\lambda|}e^{i(2k\pi+\arg(\lambda))/p}$.
Dans ce cas les polynômes $X - \mu_{\lambda,0}, \dots, X - \mu_{\lambda,p-1}$ sont deux à deux premiers entre eux et de produit $X^p - \lambda$. Et donc d'après le lemme des noyaux :
$\mathcal{M}_{n,1}(\mathbb{C}) = \bigoplus_{\lambda\in \mathrm{Sp}(B^p)} \left(\bigoplus_{k=0}^{p-1} \ker(B - \mu_{\lambda,k}\mathrm{Id})\right) = \bigoplus_{\mu\in \mathrm{Sp}(B)} \ker(B - \mu \mathrm{Id})$.
càd B est diagonalisable (il n'y a pas trop de termes, certains des noyaux en jeu sont nuls).

Le résultat n'est plus vrai pour $n, p \geq 2$ si on ne suppose plus A inversible. Par exemple pour $A = 0$ il suffit de trouver une matrice non nulle nilpotente d'indice inférieur à p.
$B = \left(\begin{array}{ccc|c} 0 & \cdots & 0 & 1 \\ \hline & & & 0 \\ & 0 & & \vdots \\ & & & 0 \end{array}\right)$ convient car $B^2 = 0$.

XIII.3.6 Diagonalisabilité de f dans le cas f^2 diagonalisable

[Enoncé]

1. Remarquons que l'on a toujours $\ker(f) \subset \ker(f^2)$. Supposons que f est diagonalisable.
   Il existe une base $\mathcal{B}$ de $\mathbb{C}^n$ telle que $\mathrm{Mat}_{\mathcal{B}}(f) = \mathrm{diag}(0, \dots, 0, \lambda_1, \dots, \lambda_r)$ avec $r = \mathrm{rg}(f)$.
   Alors $\mathrm{Mat}_{\mathcal{B}}(f^2) = \mathrm{Mat}_{\mathcal{B}}(f)^2 = \mathrm{diag}(0, \dots, 0, \lambda_1^2, \dots, \lambda_r^2)$. Donc $\mathrm{rg}(f^2) = r = \mathrm{rg}(f)$ d'où d'après le théorème du rang $\dim(\ker f) = \dim(\ker f^2)$. Donc $\ker(f) = \ker(f^2)$.
   Réciproquement supposons que f^2 est diagonalisable et que $\ker(f) = \ker(f^2)$.
   Alors $\mathbb{C}^n = \ker(f^2) \oplus \bigoplus_{\lambda\in \mathrm{Sp}(f^2)\setminus\{0\}} \ker(f^2 - \lambda \mathrm{Id}_{\mathbb{C}^n})$.
   Or $\forall \lambda \in \mathrm{Sp}(f^2)\setminus\{0\}$, $\exists \mu \in \mathbb{C}^*,\ \lambda = \mu_\lambda^2$.
   Dans ce cas les polynômes $X - \mu_\lambda$ et $X + \mu_\lambda$ sont premiers entre eux et de produit $X^2 - \lambda$.
   Et donc d'après le lemme des noyaux :
   $\mathbb{C}^n = \ker(f) \oplus \bigoplus_{\lambda\in \mathrm{Sp}(f^2)\setminus\{0\}} \ker(f - \mu_\lambda \mathrm{Id}_{\mathbb{C}^n}) \oplus \ker(f + \mu_\lambda \mathrm{Id}_{\mathbb{C}^n}) = \bigoplus_{\mu\in \mathrm{Sp}(f)} \ker(f - \mu \mathrm{Id}_{\mathbb{C}^n})$.
   càd f est diagonalisable (il n'y a pas trop de termes, certains des noyaux en jeu sont nuls).

   Remarque : la même preuve montre que pour tout $p \in \mathbb{N}^*$ f est diagonalisable si et seulement si f^p est diagonalisable et $\ker f = \ker f^p$.
2. Si $\mathrm{Sp}(f^2) \subset \mathbb{R}_+$ alors on peut faire la même preuve pour montrer que $\ker f = \ker f^2 \implies$ f diagonalisable. Montrons que cette condition est nécessaire.

Supposons que f est diagonalisable. Alors dans une base $\mathcal{B}$ de diagonalisation de f, $\mathrm{Mat}_{\mathcal{B}}(f^2) = \mathrm{diag}(\lambda_1^2, \dots, \lambda_n^2)$ avec $\lambda_1, \dots, \lambda_n$ des valeurs propres de f. Comme f est un endomorphisme d'un $\mathbb{R}$-espace vectoriel, ses valeurs propres sont toutes réelles. Ainsi $\forall i \in [\![1;n]\!],\ \lambda_i^2 \geq 0$ et par suite $\mathrm{Sp}(f^2) \subset \mathbb{R}_+$.

3. Quitte à considérer l'endomorphisme $f_A \in \mathbb{K}^n$ induit par A, les questions précédentes montrent que si A^2 est diagonalisable dans $\mathcal{M}_n(\mathbb{K})$ alors A est diagonalisable dans $\mathcal{M}_n(\mathbb{C})$ ssi $\ker A = \ker A^2$ et A est diagonalisable dans $\mathcal{M}_n(\mathbb{R})$ ssi $\ker A = \ker A^2$ et $\mathrm{Sp}(A^2) \subset \mathbb{R}_+$.
On note $(e_1, \dots, e_n)$ la base canonique de $\mathbb{K}^n$.
On calcule $Ae_i = a_i e_{n+1-i}$ donc $A^2 e_i = a_i a_{n+1-i} e_i$. Donc A^2 est diagonalisable dans $\mathcal{M}_n(\mathbb{K})$.
De plus $\ker A = \mathrm{Vect}(e_i \mid a_i = 0)$ et $\ker A^2 = \mathrm{Vect}(e_i \mid a_i a_{n-i+1} = 0)$. Ainsi $\ker A = \ker A^2 \iff (\forall i \in [\![1;n]\!],\ a_i = 0 \iff a_i a_{n-1+i} = 0) \iff (\forall i \in [\![1;n]\!],\ a_i = 0 \iff a_{n+1-i} = 0)$.

   Pour $\mathbb{K} = \mathbb{C}$:
   A est diagonalisable ssi $\forall i \in [\![1;n]\!],\ a_i = 0 \iff a_{n+1-i} = 0$.

   Pour $\mathbb{K} = \mathbb{R}$:
   Il faut et il suffit de plus que les produits $a_i a_{n+1-i}$ soient positifs, autrement dit que a_i et a_{n+1-i} soient de même signes lorsqu'ils sont non nuls.

XIII.3.7 Endomorphismes diagonalisables non bijectifs

[Enoncé]

1. On écrit $P(X) = XQ(X)$. Comme 0 est racine simple de P on sait que $X \wedge Q(X) = 1$. Par conséquent d'après le lemme des noyaux $E = \mathrm{Ker}P(f) = \mathrm{Ker}f \bigoplus \mathrm{Ker}Q(f)$. Montrons que $\mathrm{Ker}Q(f) = \mathrm{Im}f$. On note $Q(X) = \sum_{k=0}^{d} a_k X^k$. On sait que $a_0 \neq 0$.

   Soit $y \in \mathrm{Im}f$. $\exists x \in E,\ y = f(x)$. Donc $Q(f)(y) = \sum_{k=0}^{d} a_k f^{k+1}(x) = (f \circ Q(f))(x) = P(f)(x) = 0$. Donc $y \in \mathrm{Ker}Q(f)$.

   Réciproquement, fixons $x \in \mathrm{Ker}Q(f)$. $Q(f)(x) = 0 \iff -a_0 x = \sum_{k=1}^{d} a_k f^k(x) \iff x = f\left(-\frac{1}{a_0}\sum_{k=0}^{d-1} a_{k+1} f^k(x)\right)$. Donc $x \in \mathrm{Im}f$.
   Ainsi $\mathrm{Ker}Q(f) = \mathrm{Im}f$ et par suite $E = \mathrm{Ker}f \bigoplus \mathrm{Im}f$.

   Remarque : si E est de dimension finie le théorème du rang donne $\dim(\mathit{Ker}Q(f)) = \mathrm{rg}(f)$ *donc il suffit de vérifier une seule inclusion.*

2. Comme f n'est pas injectif, 0 est valeur propre de f càd $\pi_f(0) = 0$. De plus f est diagonalisable donc π_f est scindé à racines simples. Donc $\pi'_f(0) \neq 0$. Enfin π_f est un polynôme annulateur de f donc d'après la question précédente $E = \mathrm{Ker} f \bigoplus \mathrm{Im} f$.

XIII.3.8 Valuation du polynôme minimal

[Enoncé]

1. Si $p = 0$ alors $\pi_f(0) \neq 0$ càd 0 n'est pas valeur propre de f càd, comme E est dimension finie, f est bijectif.
2. C'est la même preuve que dans l'exercice précédant.
   On écrit $\pi_f(X) = X^p Q(X)$. Comme p est la valuation de π_f on sait que $X^p \wedge Q(X) = 1$.
   Par conséquent d'après le lemme des noyaux $E = \mathrm{Ker}\pi_f(f) = \mathrm{Ker}(f^p) \bigoplus \mathrm{Ker} Q(f)$.
   Montrons que $\mathrm{Ker} Q(f) = \mathrm{Im}(f^p)$. On note $Q(X) = \sum_{k=0}^{d} a_k X^k$. On sait que $a_0 \neq 0$.
   Soit $y \in \mathrm{Im}(f^p)$. $\exists x \in E,\ y = f^p(x)$. Donc $Q(f)(y) = \sum_{k=0}^{d} a_k f^{k+p}(x) = (f^p \circ Q(f))(x) = \pi_f(f)(x) = 0$. Donc $y \in \mathrm{Ker} Q(f)$.
   De plus d'après le théorème du rang, $\mathrm{rg}(f^p) = \dim(E) - \dim \mathrm{Ker}(f^p) = \dim \mathrm{Ker}(Q(f))$.
   Ainsi $\mathrm{Ker} Q(f) = \mathrm{Im}(f^p)$ et par suite $E = \mathrm{Ker}(f^p) \bigoplus \mathrm{Im}(f^p)$.
3. Soit $q \in \mathbb{N}^*$ tel que $E = \mathrm{Ker}(f^q) \bigoplus \mathrm{Im}(f^q)$. Notons R le polynôme minimal de l'endomorphisme $\tilde{f}$ induit par f sur $\mathrm{Im}(f^q)$. Alors $X^q R(X)$ annule f sur $\mathrm{Ker}(f^q)$ et sur $\mathrm{Im}(f^q)$ donc sur E. Ainsi $\pi_f | X^q R(X)$ et donc $X^p | X^k \pi_f$.
   Or comme $\mathrm{Ker}(f^q)$ et $\mathrm{Im}(f^q)$ sont en somme directe,
   $$\mathrm{Ker}(\tilde{f}) = \mathrm{Ker}(f) \cap \mathrm{Im}(f^q) \subset \mathrm{Ker}(f^q) \cap \mathrm{Im}(f^q) = \{0\}$$
   Autrement dit 0 n'est pas racine de R d'où $X^p | X^q$ i.e $p \leq q$.

XIII.3.9 Sous-espaces stables

[Enoncé]
Considérons l'endomorphisme u_F induit par u sur F.
Pour tout polynôme $Q \in \mathbb{K}[X]$, $Q(u_F)$ est exactement l'endomorphisme induit par $Q(u)$ sur F. Donc $\forall Q \in \mathbb{K}[X],\ \ker Q(u_F) = F \cap \ker Q(u)$.
$P(u) = 0 \implies P(u_F) = 0$.
Donc d'après le lemme des noyaux $F = \ker P(u_F) = \bigoplus_{i=1}^{r} \ker(P_i^{\alpha_i}(u_F)) = \bigoplus_{i=1}^{r} F \cap N_i$.

XIII.3.10 Une formule sur les polynômes

[Enoncé]
On considère l'endomorphisme de $S \in Ł(\mathbb{C}_{n-1}[X])$ défini par $\forall P \in \mathbb{C}_{n-1}[X],\ S(P) =$

$P(X+1)$.
Alors l'égalité se réécrit

$$\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}S^k = 0$$

Ou encore

$$(S-\mathrm{Id})^n = 0$$

Il suffit donc de montrer que $S-\mathrm{Id}$ est nilpotent (on dit que S est unipotent) et le théorème de Cayley-Hamilton permettra de conclure.
Soit λ une valeur propre de $S-\mathrm{Id}$ et P un vecteur propre associé (que l'on peut prendre unitaire). On note $P(X) = X^d + Q(X)$ avec $d = \deg(P)$ (et $\deg(Q) < d$).
Alors $(S-\mathrm{Id})(P) = (X+1)^d - X^d + Q(X+1) - Q(X) = \sum_{k=0}^{d-1}\binom{d}{k}X^k + Q(X+1) - Q(X)$.
On en déduit que $\deg((S-\mathrm{Id})(P)) \leq d-1 < \deg(P)$. Or $(S-\mathrm{Id})(P) = \lambda P$ donc si $\lambda \neq 0$, $\deg((S-\mathrm{Id})(P)) = \deg(P)$. Par conséquent $\lambda = 0$.
Ainsi $S-\mathrm{Id}$ est un endomorphisme nilpotent de $\mathbb{C}_{n-1}[X]$ qui est un $\mathbb{C}$-espace vectoriel de dimension n, son polynôme caractéristique est donc X^n.
En outre, d'après le théorème de Cayley-Hamilton $(S-\mathrm{Id})^n = 0$.

XIII.3.11 Ordre de matrice

[Enoncé]
Soit $M \in GL_2(\mathbb{Z})$ d'ordre fini que l'on note k. On note λ et μ ses valeurs propres. Puisque M est d'ordre fini, on en déduit que λ et μ sont des racines k-ème de l'unité, en particulier $|\lambda| = |\mu| = 1$. Par conséquent, on en déduit que

$$|d| = |\lambda||\mu|$$
$$|t| = |\lambda+\mu| \leq |\lambda| + |\mu| = 2$$

Donc

$$d = \pm 1$$
$$t \in [\![-2;2]\!]$$

Si $d = 1$, on en déduit que $\mu = \frac{1}{\lambda} = \overline{\lambda}$. Par conséquent, $t = 2\mathrm{Re}(\lambda)$.
Ainsi $\mathrm{Re}(\lambda) \in \{0, \pm\frac{1}{2}, \pm 1\}$. On en déduit donc les couples suivants (à l'ordre près entre λ et μ) :

$$(i,-i);(j,j^2);(-j,-j^2);(1,1) \text{ et } (-1,-1)$$

Dans les trois premiers cas, M est diagonalisable et l'on obtient respectivement les ordres 4, 3 et 6.
Dans les cas, où $\lambda = \mu = \pm$, M est semblable à une matrice de la forme

$$\begin{pmatrix} \pm 1 & a \\ 0 & \pm 1 \end{pmatrix}$$

On remarque que A est d'ordre fini si et seulement si $a = 0$.
Pour $\lambda = \mu = 1$, A est d'ordre 1, et pour $\lambda = \mu = -1$, A est d'ordre 2.
Si $d = -1$, on en déduit $\mu = \frac{-1}{\lambda} = -\overline{\lambda}$. Par conséquent, $t = 2i\mathrm{Im}(\lambda) \in \mathbb{Z}$.
On en déduit que $\mathrm{Im}(\lambda) = 0$ Ainsi, $\lambda = 1$ et $\mu = -1$ ou $\lambda = -1$ et $\mu = 1$, dans les cas, on obtient des matrices diagonalisables d'ordre 2. Ainsi, les ordres possibles sont 1,2,3,4 et 6.

Ordre	Matrice
1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
2	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
3	$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$
4	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
6	$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$

XIII.3.12 Sous-groupes finis de $\mathrm{GL}_2(\mathbb{Z})$

[Enoncé]

1. On montre que $\mathcal{M}_2(\mathbb{Z})$ est un sous-anneau de $\mathcal{M}_2(\mathbb{C})$, ce qui découle directement du fait que $\mathbb{Z}$ est un anneau.
   $\mathrm{GL}_2(\mathbb{Z})$ est l'ensemble des inversibles d'un anneau, c'est donc un groupe.
   Il sera utile pour la suite de remarquer que si $M \in \mathrm{GL}_2(\mathbb{Z})$ alors $\det(M) \in \{-1, 1\}$. En effet le déterminant est polynomial en les coefficients de la matrices et $\mathbb{Z}$ est un anneau donc $M \in \mathrm{GL}_2(\mathbb{Z}) \implies \det(M) \in \mathbb{Z}$ et $\det(M^{-1}) = \det(M)^{-1} \in \mathbb{Z}$. $\det(M)$ est donc un inversible de $\mathbb{Z}$, d'où $\det(M) \in \{-1, 1\}$.
2. Notons $n = |G|$. Fixons $M \in G$. On sait que $M^n = I_2$ et le polynôme $X^n - 1$ est scindé à racines simples sur $\mathbb{C}$. Donc M est diagonalisable dans $\mathcal{M}_n(\mathbb{C})$ et de plus, $\mathrm{Sp}(M) \subset \mathbb{U}_n$. On note $M = P \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} P^{-1}$ avec $P \in \mathrm{GL}_2(\mathbb{C})$.
   Supposons que λ est réel i.e $\lambda \in \{-1, 1\}$. Alors $\det(M) = \lambda\mu \in \{-1, 1\}$ donne $\mu \in \{-1, 1\}$. De même $\mu \in \mathbb{R} \implies (\mu, \lambda) \in \{-1, 1\}^2$. Dans ce cas, $M^2 = I_2$.
   On suppose dans la suite que λ et μ ne sont pas réels. Les coefficients du polynôme caractéristique de M sont polynomiaux en ceux de M, ce sont donc des entiers et a fortiori $\chi_M \in \mathbb{R}[X]$. Ainsi $\mu = \overline{\lambda}$. On note aussi $\lambda = e^{i\theta}$ avec $\theta \in]-\pi, \pi]$.
   On en déduit que $\mathrm{Tr}(M) = \lambda + \overline{\lambda} = 2\cos(\theta)$. Or $\mathrm{Tr}(M) \in \mathbb{Z}$ puisque $M \in \mathcal{M}_n(\mathbb{Z})$.
   Par conséquent $2\cos(\theta) \in [-2, 2] \cap \mathbb{Z}$ donc $\cos(\theta) \in \left\{-1, -\frac{1}{2}, 0, \frac{1}{2}, 1\right\}$.
   $\cos(\theta) = 1 \implies \theta = 0 \implies \lambda = 1$ et $\cos(\theta) = -1 \implies \theta = \pi \implies \lambda = -1$. Ces deux cas sont exclus.

$\cos(\theta) = 0 \implies \theta \in \left\{-\frac{\pi}{2}, \frac{\pi}{2}\right\} \implies \lambda \in \{i, -i\} \implies M^4 = I_2.$
$\cos(\theta) = \frac{1}{2} \implies \theta \in \left\{-\frac{\pi}{3}, \frac{\pi}{3}\right\} \implies \lambda \in \{e^{i\pi}/3, e^{-i\pi/3}\} \implies M^6 = I_2.$
$\cos(\theta) = -\frac{1}{2} \implies \theta \in \left\{-\frac{2\pi}{3}, \frac{2\pi}{3}\right\} \implies \lambda \in \{e^{2i\pi/3}, e^{-2i\pi/3}\} \implies M^3 = I_2.$
Ainsi dans tous les cas $M^{\text{ppcm}(2,3,4,6)} = M^{12} = I_2$.

XIII.3.13 Sous-groupes finis de $\mathrm{GL}_n(\mathbb{Z})$

[Enoncé]

1. $\det M$ est polynomial en les coefficients de M. Comme $\mathbb{Z}$ est un anneau, $\det M \in \mathbb{Z}$. Ainsi si $|\det M| = 1$ alors $\det M \in \{-1, 1\}$ et $M \in \mathrm{GL}_n(\mathbb{C})$. De plus, $M^{-1} = \frac{1}{\det(M)} \mathrm{Com}(M)^\top = \pm \mathrm{Com}(M)^\top$. Or les coefficients de $\mathrm{Com}(M)$ sont polynomiaux en ceux de M puisque ce sont des déterminants de matrices extraites de M. Les coefficients de $\mathrm{Com}(M)^\top$ sont ceux de $\mathrm{Com}(M)$ donc $M^{-1} \in \mathcal{M}_n(\mathbb{Z})$.
Réciproquement, si $M \in \mathrm{GL}_n(\mathbb{Z})$ alors $\det M$ et $\det M^{-1} = \frac{1}{\det M}$ sont des entiers. Ainsi $\det M \in \{-1, 1\}$ et a fortiori $|\det M| = 1$.
On a vu que $\mathrm{GL}_n(\mathbb{Z}) = \det^{-1}(\{-1, 1\})$. Or $\det : \mathrm{GL}_n(\mathbb{C}) \to \mathbb{C}^*$ est un morphisme de groupes. $\{-1, 1\}$ est un sous-groupe de $\mathbb{C}^*$, $\mathrm{GL}_n(\mathbb{Z})$ est donc un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$.

2. a. $\forall k \in \mathbb{N},\ N^k = \frac{1}{3^k} \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} M^j$.

   1ère méthode :
   Comme G est un groupe fini $M^{|G|} = I_n$. Par conséquent l'ensemble $\langle M \rangle = \{M^j,\ j \in \mathbb{Z}\}$ est fini. On pose $R = \max\{\|X\|,\ X \in \langle M \rangle\}$ pour une norme quelconque de $\mathcal{M}_n(\mathbb{C})$.
   On peut majorer $\forall k \in \mathbb{N},\ \left\|N^k\right\| \leq \frac{R}{3^k} \sum_{j=0}^{k} \binom{k}{j} = R\left(\frac{2}{3}\right)^k \underset{k\to+\infty}{\longrightarrow} 0$.
   Ainsi la suite $(N^k)_{k\in\mathbb{N}}$ converge vers la matrice nulle.
   2ème méthode :
   Comme G est un groupe fini, $M^{|G|} = I_n$. le polynôme $X^{|G|} - 1$ est scindé à racines simples sur $\mathbb{C}$ donc M est diagonalisable sur $\mathbb{C}$ et de plus $\mathrm{Sp}(M) \subset \mathbb{U}_{|G|}$.
   On écrit $M = PDP^{-1}$ avec $P \in \mathrm{GL}_n(\mathbb{C})$ et $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$.
   Alors $N^k = P\,\mathrm{diag}\left(\left(\frac{\lambda_1 - 1}{3}\right)^k, \ldots, \left(\frac{\lambda_n - 1}{3}\right)^k\right) P^{-1}$.
   Or $\forall \lambda \in \mathbb{U},\ \left|\frac{\lambda - 1}{3}\right| \leq \frac{2}{3}$. Donc $D^k \underset{k\to+\infty}{\longrightarrow} 0$. Enfin l'application $A \mapsto PAP^{-1}$ est linéaire sur $\mathcal{M}_n(\mathbb{C})$, qui est un espace-vectoriel de dimension finie, donc continue. On en déduit que $N^k \underset{k\to+\infty}{\longrightarrow} 0$.

b. On va montrer que l'application π_G est injective. Comme $\mathcal{M}_n(\mathbb{Z}/3\mathbb{Z})$ est un ensemble fini, on obtiendra que $\mathrm{GL}_n(\mathbb{Z})$ est fini.
On montre aisément que π est un morphisme d'anneau, il induit donc un morphisme de groupes $\tilde{\pi}$ de G dans $\pi(G)$. Fixons $A \in \ker\tilde{\pi}$.
$\tilde{\pi}(A) = \overline{I}_n \iff \exists N \in \mathcal{M}_n(\mathbb{Z}),\ A - I_n = 3N$.
D'après la question précédente $(N^k)_{k\in\mathbb{N}}$ converge vers 0. Donc en notant M_{ij} le coefficient (i,j) d'une matrice M, chacune des suites $(N^k_{ij})_{k\in\mathbb{N}}$ converge vers 0. Or ce sont des suites d'entiers, elles stationnent donc à 0. On en déduit qu'il existe $d \in \mathbb{N}^*$ tel que $N^d = 0$ i.e $(A - I_n)^d = 0$. Montrons que cela impose $A = I_n$.
On a vu que A est diagonalisable. Notons $A = QD'Q^{-1}$ avec $Q \in \mathrm{GL}_n(\mathbb{C})$ et $D' = \mathrm{diag}(\mu_1, \dots, \mu_n)$. Alors $(A - I_n)^d = 0 \iff (D' - I_n)^d = 0 \iff \forall i \in [\![1;n]\!],\ (\mu_i - 1)^d = 0, \iff \forall i \in [\![1;n]\!],\ \mu_i = 1 \iff A = I_n$.
Ainsi $\tilde{\pi}$ est injectif et donc $|G| \leq |\mathcal{M}_n(\mathbb{Z}/3\mathbb{Z})| = 3^{n^2}$.

XIII.3.14 Isomorphisme entre $\mathbf{GL}_n(\mathbb{C})$ et $\mathbf{GL}_m(\mathbb{C})$

[Enoncé]
On va travailler avec les endomorphismes φ_i canoniquement associés aux matrices A_i.

1. a. φ_1 est diagonalisable, il a donc une valeur propre λ. On note E_λ le sous-espace propre associé. Comme φ_1 et φ_2 commutent, E_λ est stable par φ_2 et φ_2 induit donc un endomorphisme $\tilde{\varphi}_2$ sur E_λ.
Comme φ_2 est diagonalisable, $\tilde{\varphi}_2$ l'est aussi. Il existe donc une base $\mathcal{B}_\lambda$ de E_λ formée de vecteurs propres de $\tilde{\varphi}_2$, donc de φ_2. Mais par définition de E_λ, les éléments de $\mathcal{B}$ sont des vecteurs propres de φ_1 (associés à la valeur propre λ). Enfin φ_1 est diagonalisable donc $\mathcal{M}_{n,1}(\mathbb{C}) = \bigoplus_{\lambda\in\mathrm{Sp}(\varphi_1)} E_\lambda$. Ainsi la base $\mathcal{B}$ de $\mathcal{M}_{n,1}(\mathbb{C})$ obtenue par concaténation des bases $\mathcal{B}_\lambda$ est une base de diagonalisation de φ_1 et φ_2.

b. Par récurrence sur le nombre d'endomorphisme : Supposons qu'il existe un entier $k \in [\![1;p]\!]$ tel que si $u_1, \dots, u_{k-1}$ sont des endomorphismes diagonalisables d'un $\mathbb{C}$-espace vectoriel de dimension inférieure à n et qui commutent deux à deux alors ils sont codiagonalisables.
φ_k est diagonalisable, il admet donc une valeur propre μ. On note E_μ le sous-espace propre associé. Chacun des φ_i commute avec φ_k, ils induisent des endomorphismes $\tilde{\varphi}_i$ sur E_μ.
Les endomorphismes $\tilde{\varphi}_1, \dots, \tilde{\varphi}_{k-1}$ sont diagonalisables et commutent deux à deux (car c'est le cas de $\varphi_1, \dots, \varphi_{k-1}$). Ainsi par hypothèse de récurrence il existe une base $\mathcal{B}_\mu$ de E_μ formée de vecteurs propres communs à $\tilde{\varphi}_1, \dots, \tilde{\varphi}_{k-1}$, donc à $\varphi_1, \dots, \varphi_{k-1}$. Par définition de E_μ, les éléments de cette base sont des vecteurs propres de φ_k. Enfin φ_k est diagonalisable donc $\mathcal{M}_{n,1}(\mathbb{C}) = \bigoplus_{\mu\in\mathrm{Sp}(\varphi_k)} E_\mu$. Ainsi la base $\mathcal{B}$ de $\mathcal{M}_{n,1}(\mathbb{C})$ obtenue par concaténation des bases $\mathcal{B}_\mu$ est une base de diagonalisation commune à $\varphi_1, \dots, \varphi_k$.

2. Soit $A \in G$. Le polynôme $X^2 - 1 = (X-1)(X+1)$ annule A donc A est diagonalisable et ses valeurs propres valent -1 ou 1. Il n'y a qu'un nombre fini de choix possibles
On montre cf.[l'exo qui va bien] que comme G est un groupe dont tous les éléments sont d'ordre au plus 2, G est un groupe commutatif.
Considérons $V = \text{Vect}(G)$. V est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{C})$, il est donc de dimension finie r. Donnons nous $A_1, \dots, A_r$ une base de $\text{Vect}(G)$. Comme $A_1, \dots, A_r$ commutent deux à deux, la question 1 assure l'existence d'une matrice inversible P telle que pour tout $i \in [\![1; r]\!]$, la matrice $D_i = P^{-1}A_iP$ est diagonale.
Donc si $A \in G$, on peut écrire $A = \sum_{i=1}^{r} a_i A_i$ d'où $P^{-1}AP = \sum_{i=1}^{r} a_i D_i$ est diagonale. On en déduit que G s'injecte par $\iota : A \mapsto P^{-1}AP$ dans le groupe $D_n = \{\text{diag}(\varepsilon_1, \dots, \varepsilon_n),\ (\varepsilon_1, \dots, \varepsilon_n) \in \{-1, 1\}^n\}$ qui est un ensemble fini. G est donc fini. De plus l'injection donne $|G| \leq 2^n$.

   Remarque : Ce ne sera pas utile pour la suite mais on peut préciser la réponse. L'injection ι est un morphisme de groupes, G est donc isomorphe à un sous-groupe de D_n. Par le théorème de Lagrange le cardinal de G divise 2^n, c'est donc une puissance de 2 inférieure à 2^n.

3. Supposons que l'on dispose d'un isomorphisme $\varphi : \text{GL}_n(\mathbb{C}) \to \text{GL}_m(\mathbb{C})$. Notons pour $k \in \mathbb{N}^*$, G_k la partie de $\text{GL}_k(\mathbb{C})$ formée des matrices A telles que $A^2 = I_k$.
$\forall A \in G_n,\ \varphi(A)^2 = \varphi(A^2) = \varphi(I_n) = I_m$. Donc $\varphi(G_n) \subset G_m$. Et de même, $\varphi^{-1}(G_m) \subset G_n$ d'où $G_m \subset \varphi(G_n)$. Ainsi $G_m = \varphi(G_n)$. En particulier, $\varphi(D_n)$ est un sous-groupe de $\text{GL}_m(\mathbb{C})$ inclus dans G_m, d'après la question précédente $2^n = |D_n| = |\varphi(D_n)| \leq 2^m$. De même, $\varphi^{-1}(D_m)$ est un sous-groupe de $\text{GL}_n(\mathbb{C})$ inclus dans G_n, donc $2^m = |D_m| = |\varphi^{-1}(D_m)| \leq 2^n$. Ainsi $2^n = 2^m$ et par suite $n = m$.

XIII.3.15 Inverse et conjugaison

[Enoncé]

Supposons que $\exists S \in \text{GL}_n(\mathbb{C}),\ A = S\overline{S}^{-1}$. On montre que $\forall A, B \in \mathcal{M}_n(\mathbb{C}),\ \overline{AB} = \overline{A} \times \overline{B}$.
$SS^{-1} = I_n$ donc en passant au conjugué $\overline{S}\ \overline{S^{-1}} = I_n$ i.e $\overline{S}^{-1} = \overline{S^{-1}}$.
Donc $A\overline{A} = S\overline{S}^{-1}\overline{S}S^{-1} = I_n$.

Réciproquement supposons que $A\overline{A} = I_n$. On note $X, Y \in \mathcal{M}_n(\mathbb{R})$ telles que $A = X + iY$. Alors $A = X - iY$.
On a donc $(X+iY)(X-iY) = I_n$ c'est à dire $X^2 + Y^2 + i(YX - XY) = I_n$. En identifiant partie réelle et partie imaginaire on obtient $X^2 + Y^2 = I_n$ et $XY = YX$.
X et Y sont trigonalisables dans $\mathcal{M}_n(\mathbb{C})$ et comme elles commutent, on montre classiquement qu'elles trigonalisent dans une même base. On note alors $P \in \text{GL}_n(\mathbb{C})$ ainsi que T_X et T_Y triangulaires supérieures telles que $X = PT_XP^{-1}$ et $Y = PT_YP^{-1}$.
Donc d'après l'autre égalité $P(T_X^2 + T_Y^2)P^{-1} = I_n$ d'où $T_X^2 + T_Y^2 = I_n$.
Montrons que les valeurs propres de A sont toutes de modules 1. Soit $\lambda \in \text{Sp}(A)$ de module maximal et x un vecteur propre associé. $Ax = \lambda x \implies \overline{A}\ \overline{x} = \overline{\lambda}\ \overline{x} \implies \overline{\lambda} \in \text{Sp}(\overline{A})$. Or

$\overline{A} = A^{-1}$ et $\mathrm{Sp}(A^{-1}) = \left\{\dfrac{1}{\mu},\ \mu \in \mathrm{Sp}(A)\right\}$.
Donc $\dfrac{1}{\overline{\lambda}} \in \mathrm{Sp}(A)$. Or $\left|\dfrac{1}{\overline{\lambda}}\right| = \dfrac{1}{|\lambda|}$.

XIII.3.16 Matrice compagnon (2)

[Enoncé]

1. Il y a plusieurs méthodes plus ou moins rapides et astucieuses qui sont détaillées dans l'exercice [Matrice compagnon (1)] **(Je propose de faire les trois méthodes, récurrence, développer une grosse formule et la spéciale Gastaud que je mets là, dans le premier exo seulement)**. On se contentera ici de la plus rapide.

$$\begin{aligned}
\chi_A(X) &= \begin{vmatrix} X & 0 & \cdots & 0 & a_0 \\ -1 & \ddots & \ddots & \vdots & a_1 \\ 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & X & a_{n-2} \\ 0 & \cdots & 0 & -1 & X + a_{n-1} \end{vmatrix}_n \\
\left(L_1 \leftarrow \sum_{k=1}^{n} X^{k-1} L_k\right) \quad &= \begin{vmatrix} 0 & 0 & \cdots & 0 & P(X) \\ -1 & X & \ddots & \vdots & a_1 \\ 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & X & a_{n-2} \\ 0 & \cdots & 0 & -1 & X + a_{n-1} \end{vmatrix}_n \\
&= (-1)^{n+1} P(X) \begin{vmatrix} -1 & X & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & X \\ 0 & \cdots & \cdots & 0 & -1 \end{vmatrix}_{n-1} \\
&= P(X)
\end{aligned}$$

2. D'après le théorème de Cayley-Hamilton $\chi_A(A) = 0$ donc $\pi_A | \chi_A$. π_A et χ_A étant unitaires, il suffit de montrer $\deg(\chi_A) = n \leq \deg(\pi_A)$. Notons $(e_1, \ldots, e_n)$ la base canonique de $\mathbb{K}^n$. On remarque que $\forall i \in [\![1; n-1]\!]$, $Ae_i = e_{i+1}$ i.e $\forall i \in [\![0; n-1]\!]$, $A^i e_1 = e_i$.
Donc la famille $(A^i e_1)_{0 \leq i \leq n-1}$ est libre, et par suite c'est une base de $\mathbb{K}^n$. Montrons alors que la famille $(A^i)_{0 \leq i \leq n-1}$ est libre dans $\mathbb{K}[A]$.

Soit $(\alpha_0, \dots, \alpha_{n-1}) \in \mathbb{K}^n$, $\sum_{i=0}^{n-1} \alpha_i A^i = 0$.

Alors $\sum_{i=0}^{n-1} \alpha_i A^i e_1 = 0$ d'où $\alpha_0 = \cdots = \alpha_{n-1} = 0$. On en déduit que $\dim(\mathbb{K}[A]) \geq n$. Or d'après le cours $\dim(\mathbb{K}[A]) = \deg(\pi_A)$. Ainsi $\deg(\pi_A) \geq \deg(\chi_A)$ et on conclut que $\pi_A = \chi_A$.

3. Soit λ une valeur propre de $A^\top$ et $X = \begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix}$ un vecteur propre associé.

$$A^\top X = \lambda X \iff \begin{cases} \forall k \in [\![0; n-2]\!],\ x_{k+1} = \lambda x_k \\ \sum_{k=0}^{n-1} -a_k x_k = \lambda x_{n-1} \end{cases}$$
$$\iff \begin{cases} \forall k \in [\![0; n-1]\!],\ x_k = \lambda^k x_0 \\ \left(\lambda^n + \sum_{k=0}^{n-1} \lambda^k\right) x_0 = 0 \end{cases}$$

On en déduit que le sous-espace propre associé à λ est $\mathrm{Vect}\left(\begin{pmatrix} 1 \\ \lambda \\ \vdots \\ \lambda^{n-1} \end{pmatrix}\right)$. On peut d'ailleurs remarquer que la première ligne impose $x_0 \neq 0$ (puisque sinon $X = 0$), et donc la deuxième ligne montre d'une nouvelle manière que $\chi_A = X^n = \sum_{k=0}^{n-1} X^k$.

XIII.3.17 Polynôme minimal ponctuel

[Enoncé]

XIII.3.18 Endomorphismes cycliques

[Enoncé]

XIII.3.19 Commutant d'un endomorphisme cyclique

[Enoncé]

XIII.3.20 Une démonstration de Cayley-Hamilton

[Enoncé]

XIII.3.21 Indépendance de corps du polynôme minimal

[Enoncé]

XIII.3.22 Polynôme minimal de l'inverse

[Enoncé]

XIII.3.23 Polynôme minimal de la transposée

[Enoncé]

XIII.3.24 Polynôme minimal imposé

[Enoncé]

XIII.3.25 Matrice de Gram

[Enoncé]

XIII.3.26 Matrice circulante

[Enoncé]

XIII.3.27 Diagonalisabilité du produit de deux matrices

[Enoncé]

XIII.3.28 Diagonalisation d'une matrice par bloc

[Enoncé]

XIII.3.29 Exponentielle matricielle

[Enoncé]

XIII.3.30 Exponentiel d'un endomorphisme nilpotent

[Enoncé]

XIII.3.31 Endomorphismes anticommutants

[Enoncé]

XIII.3.32 Trace entière

[Enoncé]

XIII.3.33 $P(A)$ nilpotente

[Enoncé]

XIII.4 Correction Déterminant

XIII.4.1 Dimension de l'espace des formes multilinéaires alternées

[Enoncé]

XIII.4.2 Théorème de Bézout matriciel ★★

[Enoncé]

1. On sait que $\det(A) = \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$. Donc $\det(A)$ est polynomial en les coefficients de A.
   $\mathbb{Z}$ étant un anneau on en déduit que $\det(A) \in \mathbb{Z}$. De même $\det(B) \in \mathbb{Z}$.

2. D'après le théorème de Bézout, $\exists (u, v) \in \mathbb{Z}^2,\ u \det(A) + v \det(B) = 1$.
   On sait que $A \operatorname{Com}(A)^\top = \det(A) I_n$ et $B \operatorname{Com}(B)^\top = \det(B) I_n$.
   Ainsi $uA \operatorname{Com}(A)^\top + vB \operatorname{Com}(B)^\top = (u \det(A) + v \det(B)) I_n = I_n$. On pose alors $U = u \operatorname{Com}(A)^\top$ et $V = v \operatorname{Com}(B)^\top$.
   U et V sont des matrices carrées d'ordre n à coefficients entiers car leurs coefficients sont, au signe près, un calcul de déterminant d'une matrice extraite de A/B (donc à coefficients entiers) que multiplie u/v. Elles vérifient $AU + BV = I_n$.

XIII.4.3 Déterminant tridiagonal

[Enoncé]

XIII.4.4 Déterminant bitriangulaire ★★★

[Enoncé]

On pose $U = \begin{pmatrix} 1 & \cdots & \cdots & 1 \\ \vdots & \ddots & \iddots & \vdots \\ \vdots & \iddots & \ddots & \vdots \\ 1 & \cdots & \cdots & 1 \end{pmatrix}$ la matrice Attila.

$\forall x \in \mathbb{C}$,

$$\det(M+xU) = \begin{vmatrix} x & a+x & \dots & a+x \\ b+x & x & \ddots & \vdots \\ \vdots & \ddots & \ddots & a+x \\ b+x & \dots & b+x & x \end{vmatrix}$$

$$\underset{C_i \leftarrow C_i - C_1}{=} \begin{vmatrix} x & a & \dots & \dots & a \\ b+x & -b & a-b & \dots & a-b \\ \vdots & b & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & a-b \\ b+x & b & \dots & b & -b \end{vmatrix}$$

Donc, en développant par rapport à la première colonne, $x \mapsto \det(M+xU)$ est une fonction polynomiale de degré au plus 1.
Donc, il existe $(\lambda, \mu) \in \mathbb{C}^2$ tel que pour tout $x \in \mathbb{C}$, $\det(M+xU) = \lambda x + \mu$.
Or, $\begin{cases} \det(M-aU) = (-a)^n \\ \det(M-bU) = (-b)^n \end{cases}$ Ainsi, on en déduit que $\det(M) = \mu = \dfrac{(-a)^n b - (-b)^n a}{b-a}$.

XIII.4.5 Déterminant de Vandermonde ★

[Enoncé]
Soit $(x_1, \dots, x_{n-1}) \in \mathbb{K}^{n-1}$. On pose $f : x \mapsto V(x_1, \dots, x_{n-1}, x)$.
En développant par rapport à la dernière ligne, on remarque que f est une fonction polynomiale de degré $n-1$ de coefficient dominant $V(x_1, \dots, x_{n-1})$.
De plus, on remarque que f s'annule pour chaque x_k.
Ainsi, on en déduit que pour tout $x \in \mathbb{K}$, $f(x) = V(x_1, \dots, x_{n-1}) \prod_{k=0}^{n-1} (x - x_k)$.
Puis, en évaluant f en x_n, on a $V(x_1, \dots, x_n) = V(x_1, \dots, x_{n-1}) \prod_{k=0}^{n-1} (x_n - x_k)$.
Finalement, par récurrence, on montre que : $\forall n \in \mathbb{N}^*, V(x_1, \dots x_n) = \prod_{1 \le i < j \le n} (x_j - x_i)$.

XIII.4.6 Déterminant de Hilbert ★★★

[Enoncé]

1. a. En développant par rapport à la dernière ligne, on a : $\Delta_n(x) = \sum_{k=0}^{n-1} \dfrac{a_k}{x+k}$.

Donc en réduisant au même dénominateur, on obtient :

$$\Delta_n(x) = \frac{\displaystyle\sum_{k=0}^{n-1} a_k \prod_{\substack{0\leq i\leq n-1\\ i\neq k}} (x+i)}{x(x+1)(x+2)\dots(x+n-1)}$$

D'où l'existence d'un $Q_n = \displaystyle\sum_{k=0}^{n-1} a_k \prod_{\substack{0\leq i\leq n-1\\ i\neq k}} (x+i) \in \mathbb{R}_{n-1}[X]$ qui vérifie la condition.

b. On remarque que Δ_n s'annule pour $x \in [\![1; n-1]\!]$ donc $(X-1)\dots(X-n+1)|Q_n$. Ainsi comme $\deg((X-1)\dots(X-n+1)) = n-1 \geq \deg(Q_n)$, on sait qu'il existe $\lambda_n \in \mathbb{R}$ tel que $Q_n = \lambda_n(X-1)\dots(X-n+1)$.

2. Dans un premier temps, trouvons une expression de λ_n.

En multipliant Δ_n par $(x-n+1)$, on a : $(x-n+1)\Delta_n(x) = \begin{vmatrix} 1 & \frac{1}{2} & \frac{1}{3} & \dots & \frac{1}{n} \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \dots & \frac{1}{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{1}{n-1} & \frac{1}{n} & \frac{1}{n+1} & \dots & \frac{1}{2n-2} \\ \frac{x-n+1}{x} & \frac{x-n+1}{x+1} & \frac{x-n+1}{x+1} & \dots & 1 \end{vmatrix}$

Et donc en évaluant en $n-1$, on obtient, $\lambda_n \dfrac{(-n)(-n-1)\dots(-2n-2)}{(1-n)(2-n)\dots(-1)} = H_{n-1}$

Ainsi, $\lambda_n = \dfrac{(n-1)!}{n(n+1)\dots(2n-2)(2n-1)} H_{n-1}$.

Enfin,

$$\begin{aligned} H_n &= \frac{((n-1)!)^2}{(n\dots(2n-2))^2(2n-1)} H_{n-1} \\ &= \frac{((n-1)!)^4}{((2n-2)!)^2(2n-1)} H_{n-1} \end{aligned}$$

Par récurrence immédiate, on a :

$$\begin{aligned} H_n &= \prod_{k=1}^{n} \frac{((k-1)!)^4}{((2k-2)!)^2(2k-1)} \\ &= \prod_{k=0}^{n-1} \frac{(k!)^4}{((2k)!)^2(2k+1)!} \\ &= \frac{2^n n!}{(2n)!} \prod_{k=0}^{n-1} \frac{(k!)^4}{((2k)!)^2} \end{aligned}$$

XIII.4.7 Déterminant de Gram ★★★

[Enoncé]

On remarquera bien que p n'est pas forcément égal à n. Et qu'ici n n'est pas la dimension

de E.

1. On rappelle que pour tout $i \in [\![1;n]\!]$, $x_i = \sum_{k=1}^{n} \langle x_i, e_k \rangle e_k$. Ainsi pour tout $(i,j) \in [\![1;p]\!]$

$$\begin{aligned}(A^\top A)_{i,j} &= \sum_{k=0}^{n} \langle x_i, e_k \rangle \langle x_j, e_k \rangle \\ &= \langle x_i, \sum_{k=0}^{n} \langle x_j, e_k \rangle e_k \rangle \qquad \text{par bilinéarité du produit scalaire} \\ &= \langle x_i, x_j \rangle\end{aligned}$$

   Ainsi $G(x_1, \dots, x_p) = A^\top A$

2. Montrons que $\mathrm{Ker}(A^\top A) = \mathrm{Ker}(A)$.
   Il est clair que $\mathrm{Ker}(A) \subset \mathrm{Ker}(A^\top A)$
   Soit $X \in \mathrm{Ker}(A^\top A)$
   Donc

$$\begin{aligned} & A^\top AX = 0 \\ \text{donc} \quad & X^\top A^\top AX = 0 \\ \text{donc} \quad & \|AX\|^2 = 0 \\ \text{ainsi} \quad & AX = 0 \end{aligned}$$

   Donc, on a bien $\mathrm{Ker}(A^\top A) = \mathrm{Ker}(A)$ Finalement, $\dim(\mathrm{Ker}(G(x_1, \dots, x_p)) = \dim(\mathrm{Ker}(A))$
   Et donc, $(x_1, \dots, x_p)$ est liée ssi $\det(G(x_1, \dots, x_p)) = 0$
   Soit $x \in E$
   On note $p_{\mathcal{F}}(x)$ la projection orthogonale de x sur $\mathcal{F}$.
   Puisque $x - p_{\mathcal{F}}(x)$ appartient à l'orthogonal de $\mathcal{F}$, on remarque que :

$$G(x_1, \dots, x_p, x - p_{\mathcal{F}}(x)) = \left(\begin{array}{c|c} G(x_1, \dots, x_p) & 0_{n,1} \\ \hline 0_{1,n} & \langle x - p_{\mathcal{F}}(x), x - p_{\mathcal{F}}(x) \rangle \end{array}\right)$$

   Ainsi, puisque $\langle x - p_{\mathcal{F}}(x), x - p_{\mathcal{F}}(x) \rangle = \|x - p_{\mathcal{F}}(x)\|^2 = \mathrm{d}(x, \mathcal{F})^2$, on a $G(x_1, \dots, x_p, x - p_{\mathcal{F}}(x)) = \mathrm{d}(x, \mathcal{F})^2 G(x_1, \dots, x_p)$
   De plus, $p_{\mathcal{F}}(x) \in \mathcal{F}$, donc $\det(G(x_1, \dots, x_p, p_{\mathcal{F}}(x))) = 0$, d'après le résultat précédent.
   Finalement, par multilinéarité du déterminant, on a :

$$\det(G(x_1, \dots, x_p, x)) = \mathrm{d}(x, \mathcal{F})^2 G(x_1, \dots, x_p)$$

XIII.4.8 Déterminant de Cauchy ★★★

[Enoncé]

1. En développant par rapport à la dernière ligne, on a :
$$\begin{aligned} F(X) &= \sum_{i=1}^{n} \frac{(-1)^{n+i}}{X+b_i} C(a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n, b_1, \dots, b_n) \\ &= \frac{P(X)}{\prod_{i=1}^{n}(X+b_i)} \end{aligned}$$
avec $P(X) \in \mathbb{C}_{n-1}[X]$.
2. a. On remarque que pour tout $i \in [\![1; n-1]\!]$, $F(a_i) = 0$.
Donc il existe $\lambda \in \mathbb{C}$, tel que $P = \lambda \prod_{i=1}^{n-1}(X - a_i)$
b. En multipliant par $(X+b_n)$ la relation obtenue à la question 1, on a :
$$\frac{P(X)}{\prod_{i=1}^{n-1}(X+b_i)} = \begin{vmatrix} \frac{1}{a_1+b_1} & \cdots & \frac{1}{a_1+b_{n-1}} & \frac{1}{a_1+b_n} \\ \vdots & & \vdots & \vdots \\ \frac{1}{a_{n-1}+b_1} & \cdots & \frac{1}{a_{n-1}+b_{n-1}} & \frac{1}{a_{n-1}+b_n} \\ \frac{X+b_n}{a_n+b_1} & \cdots & \frac{X+b_n}{a_n+b_{n-1}} & 1 \end{vmatrix}$$
Donc $\dfrac{P(-b_n)}{\prod_{i=1}^{n-1}(-b_n+b_i)} = C_{n-1}$.
Et $\lambda = \dfrac{\prod_{i=1}^{n-1}(b_i - b_n)}{\prod_{i=1}^{n-1}(-b_n - a_i)} C_{n-1}$
3. Ainsi, on a : $C_n = C_{n-1} \dfrac{\prod_{i=1}^{n-1}(a_n - a_i) \prod_{i=1}^{n-1}(b_n - b_i)}{\prod_{i=1}^{n-1}(b_n + a_i) \prod_{i=1}^{n-1}(a_n + b_i)}$
Finalement, par récurrence, on obtient :
$$C_n = \frac{\prod_{1 \le i < j \le n}(a_j - a_i) \prod_{1 \le i < j \le n}(b_j - b_i)}{\prod_{1 \le i,j \le n}(a_i + b_j)}$$

XIII.4.9 Déterminant de Smith ★★★

[Enoncé]

1. $\forall j > i,\ a_{i,j} = 0$.

   Donc A est triangulaire inférieure donc $\det(A) = \prod_{i=1}^{n} a_{i,i} = 1$

2. On remarque pour tout $(i,j) \in [\![1;n]\!]^2$, $d_{i,j} = \sum_{\substack{1\leq k\leq n \\ k|i,k|j}} 1 = \sum_{k=1}^{n} a_{i,k}a_{j,k} = (A^\top A)_{i,j}$. Donc $D = A^\top A$ et donc $\det(D) = \det(A)^2 = 1$

3. On sait que $k|i \wedge j$ ssi ($k|i$ et $k|j$).
   Donc d'après l'énoncé, $i \wedge j = \sum_{k|i\wedge j} \varphi(k) = \sum_{(k|i \text{ et } k|j)} \varphi(k)$.
   Posons $P \in \mathcal{M}_n(\mathbb{R})$ tel que $p_{i,j} = \varphi(j)$ si $j|i$ et $p_{i,j} = 0$ sinon de sorte que pour tout $(i,j) \in [\![1;n]\!]^2$, $i \wedge j = \sum_{k=1}^{n} p_{i,k}a_{j,k}$.
   Ainsi, $S = PA^\top$.
   Par conséquent, $\det(S) = \prod_{k=1}^{n} \varphi(k)$

XIII.4.10 Déterminant de Cayley-Menger

[Enoncé]

XIII.5 Correction Groupes

XIII.5.1 Existence d'un idempotent ★★★

[Enoncé]
Soit $x \in E$. $\forall n \in \mathbb{N},\ x^{2^n} \in E$. Or E est fini, donc il existe $n < m$ deux entiers naturels tels que $x^{2^n} = x^{2^m}$.
Si E était un groupe de neutres e on aurait $x^{2^m-2^n} = e$, et donc $s^2 = s$ en posant $s = x^{2^m-2^n}$.
En s'inspirant de cela, on pose $s = x^{2^m-2^n}$:
Si $m = n+1$ alors $s = x^{2^n} = x^{2^m} = x^{2^{n+1}} = \left(x^{2^n}\right)^2 = s^2$.
Et si $m > n+1$, alors $s^2 = x^{2^m-2^n} \cdot x^{2^m-2^n} = x^{2^m} \cdot x^{2^m-2^n-2^n} = x^{2^n} \cdot x^{2^m-2^n-2^n} = x^{2^m-2^n} = s$. ($x^{2^m-2^n-2^n}$ a bien un sens puisque $2^m - 2^n - 2^n = 2^m - 2^{n+1} > 0$)

XIII.5.2 Sous-semi-groupes finis de $\mathcal{M}_n(\mathbb{K})$

[Enoncé]
On utilise le résultat de l'exercice précédent, ainsi on sait que U admet un idempotent que l'on note A
Donc on en déduit un polynôme annulateur de A qui est $X(X-1)$.
Par conséquent, $\mathrm{Tr}(A) = \mathrm{rg}(A) \in [\![0; n]\!]$
Ainsi, il existe une matrice A de trace appartenant à $[\![0; n]\!]$.

XIII.5.3 Groupe d'exposant inférieur à 2 ★

[Enoncé]
On remarque que tout élément $x \in G$ est une involution : $x^{-1} = x$. Fixons $(x, y) \in G^2$.
$e = (xy)^2 = xyxy = x^{-1}yxy^{-1}$ donc en multipliant par x à gauche et par y à droite on obtient $xy = yx$.

XIII.5.4 Centre et Commutant ★

[Enoncé]
On note e le neutre de G.

1. $Z(G) \subset G$.
   $(\forall x \in G,\ ex = x = xe) \implies e \in G$.
   Soit $(a, b) \in Z(G)^2$. Soit $x \in G$.
   $abx = axb = xab$ donc $ab \in Z(G)$ et $ax = xa \implies axa^{-1} = x \implies xa^{-1} = a^{-1}x$ donc $a^{-1} \in Z(G)$.
   Ainsi $Z(G)$ est un sous-groupe de G.
2. Soit $x \in G$. $\mathcal{C}(x) \subset G$.
   $ex = x = xe \implies e \in \mathcal{C}(G)$.
   Soit $(a, b) \in \mathcal{C}(G)^2$.
   $abx = axb = xab$ donc $ab \in \mathcal{C}(G)$ et $ax = xa \implies axa^{-1} = x \implies xa^{-1} = a^{-1}x$ donc

$a^{-1} \in \mathcal{C}(G)$.
Ainsi $\mathcal{C}(G)$ est un sous-groupe de G.

XIII.5.5 Théorème de Dixon ★★★★

[Enoncé]
Notons $n = |G|$. On munit $(G^2, \mathcal{P}(G^2))$ de la probabilité $\mathbb{P}$ uniforme.
On cherche à majorer la probabilité de l'évènement $A = \{(x,y) \in G^2,\ xy = yx\}$.
$$\mathbb{P}(A) = \frac{|A|}{n^2} = \frac{1}{n^2} \sum_{(x,y)\in A^2} 1 = \frac{1}{n^2} \sum_{x\in G, y\in\mathcal{C}(x)} 1 = \frac{1}{n^2} \sum_{x\in G} \sum_{y\in\mathcal{C}(x)} 1 = \frac{1}{n^2} \sum_{x\in G} |\mathcal{C}(x)|.$$
Fixons $x \in G\backslash Z(G)$. Cet ensemble est non vide puisque G n'est pas commutatif.
On sait alors que $Z(G)$ est un sous-groupe strict de $\mathcal{C}(x)$ ($x \in \mathcal{C}(x)\backslash Z(G)$) et donc que $|Z(G)| < |\mathcal{C}(x)|$.
De plus, d'après le théorème de Lagrange, $|Z(G)|$ divise $|\mathcal{C}(x)|$.
On peut donc affiner la majoration en $2|Z(G)| \leq |\mathcal{C}(x)|$. En effet, $\dfrac{|\mathcal{C}(x)|}{|Z(G)|}$ est un entier strictement supérieur à 1, il vaut donc au moins 2.
De même, $\mathcal{C}(x)$ est un sous-groupe strict de G (puisque $x \notin Z(G)$) donc $2|\mathcal{C}(x)| \leq n$.
Enfin, si $x \in Z(G)$, $\mathcal{C}(x) = G$.
On reprend le calcul,
$$\mathbb{P}(A) = \frac{1}{n^2} \sum_{x\in G} |\mathcal{C}(x)| = \frac{1}{n^2} \left(\sum_{x\in Z(G)} |G| + \sum_{x\in G\backslash Z(G)} |\mathcal{C}(x)| \right) = \frac{|Z(G)|}{n} + \frac{1}{n^2} \sum_{x\in G\backslash Z(G)} |\mathcal{C}(x)|.$$
On peut alors majorer :
$$\mathbb{P}(A) \leq \frac{|Z(G)|}{n} + \frac{1}{n^2} \sum_{x\in G\backslash Z(G)} \frac{n}{2} \leq \frac{|Z(G)|}{n} + \frac{n - |Z(G)|}{2n} \leq \frac{n + |Z(G)|}{2n} = \frac{1}{2} + \frac{|Z(G)|}{2n} \leq \frac{1}{2} + \frac{1}{8} = \frac{5}{8}$$

XIII.5.6 Opérations sur les sous-groupes ★★

[Enoncé]

1. $H \cap K \subset H \subset G$. Notons e le neutre de G
   $e \in H$ et $e \in K$ car H et K sont des sous-groupes de G.
   Soit $(a,b) \in (H \cap K)^2$.
   $ab^{-1} \in H$ et $ab^{-1} \in K$ donc $ab^{-1} \in H \cap K$.
   $H \cap K$ est un sous-groupe de G.
2. Si $H \subset K$ ou $K \subset H$ alors $H \cup K = K$ ou $H \cup K = H$. Dans tous les cas $H \cup K$ est un sous-groupe de G.
   Réciproquement supposons que $H \cup K$ est un sous-groupe de G. Supposons que $H \not\subset K$ autrement dit que $H\backslash K \neq \emptyset$.
   Il existe donc $h \in H\backslash K$. Fixons $k \in K$.
   $k \in H \cup K$ et $h \in H \cup K$ donc $hk \in H \cup K$. Si $hk \in K$ alors comme $k^{-1} \in K$, $hkk^{-1} =$

$h \in K$ ce qui est absurde.
Donc $hk \in H$. Mais alors comme $h^{-1} \in H,\ h^{-1}hk = k \in H$.
Ainsi $K \subset H$.
On a donc montré que $H \subset K$ ou $H \subset K$.

XIII.5.7 Sous-groupes finis de $\mathbb{U}$ ★★

[Enoncé]

1. Soit H un sous-groupe fini de $\mathbb{U}$.
   $\forall z \in H,\ z^{|H|} = 1 \implies H \subset \mathbb{U}_{|H|}$.
   De plus $|H| = |\mathbb{U}_{|H|}|$ donc $H = \mathbb{U}_{|H|}$.
   Les sous-groupes finis de $\mathbb{U}$ sont les $\mathbb{U}_n$ pour $n \in \mathbb{N}^*$.
2. Si $m|n$ alors il existe $k \in \mathbb{Z},\ n = mk$ et donc $\forall z \in \mathbb{U}_m,\ z^n = z^{mk} = (z^m)^k = 1^k = 1$.
   C'est à dire $\mathbb{U}_m \subset \mathbb{U}_n$.
   Si m ne divise pas n alors il existe $k \in \mathbb{Z}$ tel que k divise m et ne divise pas n et $z_k = e^{2i\pi/k} \in \mathbb{U}_m \backslash \mathbb{U}_n$:
   — $z_k^m = e^{2ia\pi} = 1$ car $a = \dfrac{m}{k} \in \mathbb{Z}$;
   — $z_k^n = e^{2ib\pi} \neq 1$ car $b = \dfrac{n}{k} \notin \mathbb{Z}$.
3. $\mathbb{U}_m \cap \mathbb{U}_n$ est un sous-groupe fini de $\mathbb{U}$ donc d'après la question 1 il existe $q \in \mathbb{N}^*$ tel que $\mathbb{U}_m \cap \mathbb{U}_n = \mathbb{U}_q$.
   Or $\mathbb{U}_m \cap \mathbb{U}_n \subset \mathbb{U}_m$ et $\mathbb{U}_m \cap \mathbb{U}_n \subset \mathbb{U}_n$ donc d'après la question 2 $q|m$ et $q|n$.
   De plus, si $k \in \mathbb{N}^*$ tel que $k|m$ et $k|n$ alors $\mathbb{U}_k \subset \mathbb{U}_m$ et $\mathbb{U}_k \subset \mathbb{U}_n$. Donc $\mathbb{U}_k \subset \mathbb{U}_m \cap \mathbb{U}_m = \mathbb{U}_q$. Ainsi d'après la question 2, $k|q$. Ainsi comme q est positif, $q = m \wedge n$.
4. D'après la question 1, il existe $r \in \mathbb{N}^*$ tel que le sous-groupe engendré par $\mathbb{U}_m \cup \mathbb{U}_n$ soit $\mathbb{U}_r$. Montrons que $r = m \vee n$.
   Par définition du sous-groupe engendré $\mathbb{U}_m \cup \mathbb{U}_n \subset \mathbb{U}_r$ c'est à dire $\mathbb{U}_m \subset \mathbb{U}_r$ et $\mathbb{U}_n \subset \mathbb{U}_r$. Donc $m|r$ et $n|r$.
   De plus, si $k \in \mathbb{N}^*$ tel que $m|k$ et $n|k$ alors $\mathbb{U}_m \cup \mathbb{U}_n \subset \mathbb{U}_k$. Donc par définition du sous-groupe engendré $\mathbb{U}_r \subset \mathbb{U}_k$ c'est à dire $r|k$. Ainsi comme r est positif, $r = m \vee n$.

XIII.5.8 Groupes quasi-cycliques de Prüfer ★★★

[Enoncé]

1. $1 = 1^{p^0} \in G_p$. Fixons $(z_1, z_2) \in G_p^2$. Il existe $k_1, k_2 \in \mathbb{N}$ tels que $z_1^{p^{k_1}} = 1 = z_2^{p^{k_2}}$.
   Donc $|z_1| = 1$ et $\left(z_1 z_2^{-1}\right)^{p^{k_1+k_2}} = \left(z_1^{p^{k_1}}\right)^{p^{k_2}} \left(z_2^{p^{k_2}}\right)^{-p^{k_1}} = 1^{p^{k_2}} \times 1^{-p^{k_1}} = 1$.
   Ainsi G_p est un sous-groupe de $\mathbb{U}$.
2. $G_p = \{z \in \mathbb{C},\ \exists k \in \mathbb{N},\ z \in \mathbb{U}_{p^k}\} = \bigcup_{k \in \mathbb{N}} \mathbb{U}_{p^k}$.

3. Montrons que les sous-groupes de G_p sont les $\mathbb{U}_{p^k}$ pour $k \in \mathbb{N}$.
   Remarquons d'abord que la suite $\left(\mathbb{U}_{p^k}\right)_{k\in\mathbb{N}}$ est croissante pour l'inclusion de sorte que si $k \in \mathbb{N}$ et si $z \notin \mathbb{U}_{p^k}$ alors $\forall i \leq k,\ z \notin \mathbb{U}_i$.
   Soit H un sous-groupe strict de G_p. Supposons par l'absurde que H est infini.
   Alors H n'est inclus dans aucun des $\mathbb{U}_{p^k}$ pour $k \in \mathbb{N}$. Autrement dit $\forall k \in \mathbb{N},\ \exists z \in H,\ z^{p^k} \neq 1$. Ou encore puisque $H \subset G_p,\ \forall k \in \mathbb{N}^*,\ \exists z \in H,\ z^{p^k} = 1 \wedge z^{p^{k-1}} \neq 1$.
   Fixons alors $k \in \mathbb{N}^*$ et $z \in H \cap \mathbb{U}_{p^k} \backslash \mathbb{U}_{p^{k-1}}$.
   L'ordre de z dans $\mathbb{U}_{p^k}$ divise l'ordre de $\mathbb{U}_{p^k}$ c'est à dire p^k. Donc comme p est premier, l'ordre de z est une puissance de p inférieure à p^k. Cependant il ne peut pas être strictement inférieur car sinon on aurait $z \in \mathbb{U}_{p^{k-1}}$. Donc z est d'ordre p^k et est un générateur de $\mathbb{U}_{p^k}$. On en déduit que $\mathbb{U}_{p^k} \subset H$. Ceci étant vrai pour tout $k \in \mathbb{N}^*$, $G_p \subset H$ puis $H = G_p$ ce qui est absurde.
   Par conséquent H est fini. Enfin, $\forall z \in H,\ z^{|H|} = 1$. C'est à dire $H \subset \mathbb{U}_{|H|}$ puis $H = \mathbb{U}_{|H|}$ puisqu'il y a égalité des cardinaux.
   On en déduit que H est cyclique.
   Pour être plus précis, H est inclus dans $\mathbb{U}_{p^r}$ pour $r \in \mathbb{N}^*$ tel que $p^r \geq |H|$. Donc $|H|$ est lui-même une puissance de p.
   Pour conclure, les $\mathbb{U}_{p^k}$ pour $k \in \mathbb{N}$ sont bien des sous-groupes de G_p.

XIII.5.9 Sous-groupes de $\mathrm{GL}_n(\mathbb{C})$ qui intersectent trivialement le groupe spécial linéaire ★★★

[Enoncé]

Considérons le morphisme $\det : G \to \mathbb{C}^*$. Par hypothèse, $\ker(\det) = G \cap \mathrm{SL}_n(\mathbb{C}) = \{I_n\}$ donc det est injectif.
Par conséquent G est isomorphe à $\mathrm{Im}(\det)$ ce que l'on note $G \simeq \mathrm{Im}(\det)$ et $\mathrm{Im}(\det)$ est un sous-groupe fini de $\mathbb{C}^*$. Notons q son ordre. $\forall z \in \mathrm{Im}(\det),\ z^q = 1 \implies \mathrm{Im}(\det) \subset \mathbb{U}_q$. Par suite, $\mathrm{Im}(\det) = \mathbb{U}_q$ par égalité des cardinaux.
Ainsi $G \simeq \mathbb{U}_q \simeq \mathbb{Z}/q\mathbb{Z}$. D'après le cours G est cyclique.

XIII.5.10 Matrices inversibles à coefficients entiers

[Enoncé]

1. Soit $M \in \mathcal{M}_n(Z)$
   Supposons que $M \in GL_n(\mathbb{Z})$
   A l'aide de la formule du déterminant, on en déduit que $\det(M) \in \mathbb{Z}$.
   On a de même $\det(M^{-1}) \in \mathbb{Z}$.
   On sait que $MM^{-1} = I_n$. Donc $\det(M)\det(M^{-1}) = \det(MM^{-1}) = 1$. Donc $\det(M) = \pm 1$
   Réciproquement, supposons que $det(M) = \pm 1$
   Immédiatement, on en déduit que M est inversible dans $\mathbb{R}$ et que $\dfrac{1}{\det(M)} \in \mathbb{Z}$.

On rappelle que $M^{-1} = \dfrac{1}{\det(M)} \mathrm{Com}(M)^\top$. Les coefficients de la comatrice sont des déterminant donc $\mathrm{Com}(M)^\top \in \mathcal{M}_n(\mathbb{Z})$.
Finalement $M^{-1} \in \mathcal{M}_n(\mathbb{Z})$ donc $\mathcal{M}_n(\mathbb{Z}) \in GL_n(\mathbb{Z})$

2. Il est clair que $I_n \in GL_n(\mathbb{Z})$
Par définition de l'ensemble, la stabilité par l'inverse est assuré.
Et soient $M, N \in GL_n(\mathbb{Z})$, $det(MN) = \det(M)\det(N) = \pm 1$. Donc $MN \in GL_n(\mathbb{Z})$

XIII.5.11 Sous-groupes de $(\mathbb{Z}, +)$ ★★

[Enoncé]

1. $\{0\} = 0\mathbb{Z}$.
2. Comme $G \neq \{0\}$, il existe $a_0 \in G \backslash \{0\}$. Alors $-a_0 \in G$ et on a toujours $a_0 > 0$ ou $-a_0 > 0$.
Ainsi $G \cap \mathbb{N}^*$ n'est pas vide. Etant une partie de $\mathbb{N}^*$ elle admet un minimum a.
3. $a \in G \implies \langle a \rangle = a\mathbb{Z} \subset G$.
4. Soit $x \in G$.
On note $x = aq + r$ la division euclidienne de x par a.
D'après la question précédente $aq \in G$ donc $r = x - aq \in G$.
Par définition de a si $r > 0$ alors $r \geq a$ ce qui est absurde.
Donc $r = 0$ c'est à dire $a|x$ c'est à dire $x \in a\mathbb{Z}$.
Ainsi $G = a\mathbb{Z}$.

XIII.5.12 Sous-groupes de $(\mathbb{R}, +)$ ★★★

[Enoncé]

1. $G \neq \{0\}$ donc il existe $a_0 \in G$ non nul. Alors $-a_0 \in G$ et on a toujours $a_0 > 0$ ou $-a_0 > 0$. Ainsi $G \cap \mathbb{R}_+^*$ est non vide.
De plus $G \cap \mathbb{R}_+^*$ est minoré, par 0 par exemple.
On en déduit que $G \cap \mathbb{R}_+^*$ admet une borne inférieure a.
2. a. $2a > a$ donc par définition de la borne inférieure il existe $x \in G \cap \mathbb{R}_+^*$ tel que $x < 2a$. De plus $x \geq a$ par définition de a et $x \neq a$ puisque $a \notin G$. Donc $x > a$ et par définition de la borne inférieure il existe $y \in G \cap \mathbb{R}_+^*$ tel que $y < x$. De même, $y > a$.
   b. On a $a < y < x < 2a$ donc $0 < x - y < 2a - a = a$. Or $x - y \in G$ puisque $x \in G$ et $y \in G$. Ceci contredit le fait que a est un minorant de $G \cap \mathbb{R}_+^*$.
   On en déduit que $a \in G$.
   c. On a déjà $\langle a \rangle = a\mathbb{Z} \subset G$. Fixons $x \in G$.
   On sait que pour $k = \lfloor \frac{x}{a} \rfloor$ on a $k \leq \dfrac{x}{a} < k + 1$

Donc $ka \leq x < (k+1)a$ puis $0 \leq x - ka < a$.
Si, $0 < x - ak < a$ alors comme $x \in G$ et $ka \in G$, $x - ak \in G$.
Ceci contredit le fait que a est un minorant de $G \cap \mathbb{R}_+^*$ donc $x - ak = 0$ c'est à dire $x = ka \in a\mathbb{Z}$.
Finalement $G = a\mathbb{Z}$.

3. Soient $\varepsilon > 0$ et $t \in \mathbb{R}$.
$a < \varepsilon$ donc $\exists x \in G,\ x \leq \varepsilon$.
De même qu'en question 2.*c* il existe $k \in \mathbb{Z}$ tel que $kx \leq t < (k+1)x$.
Alors $0 \leq t - kx < x$ et on en déduit que $|t - kx| < \varepsilon$.
Comme $kx \in G$ on a prouvé que G est dense dans $\mathbb{R}$.

Fonction (multi)périodique ★★★

On considère $P = \{T \in \mathbb{R},\ \forall x \in \mathbb{R},\ f(x+T) = f(x)\}$ l'ensemble des périodes de f.
Montrons que P est un sous-groupe de $\mathbb{R}$.
Tout d'abord $0 \in P$. Fixons $(T_1, T_2) \in P^2$. Soit $x \in \mathbb{R}$.
$f(x + T_1 - T_2) = f((x + T_1 - T_2) + T_2) = f(x + T_1) = f(x)$.
Donc $T_1 - T_2 \in P$.
Ainsi P est un sous-groupe de $\mathbb{R}$.
Donc P est soit dense dans $\mathbb{R}$ soit de la forme $a\mathbb{Z}$ avec $a \in \mathbb{R}$. Montrons que P n'est pas de la forme $a\mathbb{Z}$.
Supposons par l'absurde qu'il existe $a \in \mathbb{R}$ tel que $P = a\mathbb{Z}$.
On sait que $1 \in P$ et $\pi \in P$ donc il existe $k_1, k_2 \in \mathbb{Z}$ tels que $ak_1 = 1$ et $ak_2 = \pi$. Mais alors $a = \dfrac{1}{k_1} \in \mathbb{Q}$ d'où $\pi = ak_2 \in \mathbb{Q}$ ce qui est absurde.
Par conséquent P est dense dans $\mathbb{R}$. On peut maintenant montrer que f est constante.
Soient $x, y \in \mathbb{R}$. $\exists (T_k) \in P^{\mathbb{N}},\ \lim\limits_{k \to +\infty} T_k = y - x$.
$\forall k \in \mathbb{N},\ f(x + T_k) = f(x)$
Donc comme f est continue sur $\mathbb{R}$, par passage à la limite $f(y) = f(x + (y - x)) = f(x)$.

$\cos(\mathbb{N})$ ★★★

Montrons que $\mathbb{Z} + 2\pi\mathbb{Z}$ est dense dans $\mathbb{R}$.
$0 = 0 + 0(2\pi) \in \mathbb{Z} + 2\pi\mathbb{Z}$.
Soient $x, y \in \mathbb{Z} + 2\pi\mathbb{Z}$. $\exists a, b, c, d \in \mathbb{Z},\ x = a + 2b\pi,\ y = c + 2d\pi$.
Donc $x - y = a - c + 2(b - d)\pi \in \mathbb{Z} + 2\pi\mathbb{Z}$.
Donc $\mathbb{Z} + 2\pi\mathbb{Z}$ est un sous-groupe de $\mathbb{R}$.
Supposons qu'il existe $a \in \mathbb{R}$ tel que $\mathbb{Z} + 2\pi\mathbb{Z} = a\mathbb{Z}$.
Alors $\exists b, c \in \mathbb{Z},\ 1 = ab,\ 2\pi = ac$. Mais alors $a = \dfrac{1}{b} \in \mathbb{Q}$ d'où $\pi = \dfrac{ac}{2} \in \mathbb{Q}$ ce qui est absurde.
Par conséquent $\mathbb{Z} + 2\pi\mathbb{Z}$ est dense dans $\mathbb{R}$.
Soit $t \in [-1, 1]$. $\exists x \in \mathbb{R},\ t = \cos(x)$. $\exists (x_n) = (a_n + 2\pi b_n) \in (\mathbb{Z} + 2\pi\mathbb{Z})^{\mathbb{N}},\ x_n \underset{n \to +\infty}{\longrightarrow} x$.
Alors par continuité de cos en x, $\cos(x_n) \underset{n \to +\infty}{\longrightarrow} \sin(x)$. De plus $\forall n \in \mathbb{N},\ \sin(x_n) = \cos(a_n) =$

$\cos(|a_n|)$.
On en déduit que $\cos(|a_n|) \underset{n\to+\infty}{\longrightarrow} t$ avec $\forall n \in \mathbb{N},\ |a_n| \in \mathbb{N}$.

Valeur d'adhérence du cercle unité ★★★

Soit $z \in \mathbb{C}$. Si z est une racine de l'unité alors la suite $(z^n)_{n\in\mathbb{N}}$ stationne à 1 qui est donc sa seule valeur d'adhérence.
Supposons maintenant que z n'est pas une racine de l'unité. Cela revient à supposer, si l'on écrit $z = e^{2i\pi\theta}$ avec $\theta \in \mathbb{R}$, que $\theta \notin \mathbb{Q}$.
On va alors montrer que $\mathbb{Z} + \theta\mathbb{Z}$ est dense dans $\mathbb{R}$. On montre aisément que $\mathbb{Z} + \theta\mathbb{Z}$ est un sous-groupe de $(\mathbb{R}, +)$. Montrons qu'il n'est pas monogène. Par l'absurde on suppose qu'il existe $a \in \mathbb{R}$ tel que $\mathbb{Z} + \theta\mathbb{Z} = a\mathbb{Z}$.
Alors on sait qu'il existe un entier k tel que $1 = ak$. On en déduit que $a = \dfrac{1}{k} \in \mathbb{Q}$. Nonobstant on sait aussi qu'il existe un entier m tel que $\theta = am$. Donc $\theta \in \mathbb{Q}$ ce qui est absurde.
Ainsi $\mathbb{Z} + \theta\mathbb{Z}$ n'est pas monogène et d'après le résultat sur les sous-groupes de $(\mathbb{R}, +)$, il est dense dans $\mathbb{R}$.
On en déduit par continuité et 1-périodicité de la fonction $f : x \in \mathbb{R} \mapsto e^{2i\pi x}$ que $f(\mathbb{Z}+\theta\mathbb{Z}) = \{e^{2ki\pi\theta},\ k \in \mathbb{Z}\} = \{e^{2in\pi\theta},\ n \in \mathbb{N}\} = \{z^n,\ n \in \mathbb{N}\}$ est dense dans $f(\mathbb{R}) = \mathbb{U}$.
En particulier 1 est une valeur d'adhérence de la suite $(z^n)_{n\in\mathbb{N}}$.

XIII.5.13 Sous-groupes distingué

[Enoncé]

1. Soit $g \in G$ soit $h \in Z(G)$.
$$ghg^{-1} = hgg^{-1} = h \in Z(G)$$
Donc $Z(G)$ est distingué dans G.
2. Soit $g \in G$ soit $h \in \mathrm{Ker}(f)$.
$$f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)ef(g)^{-1} = e$$
Donc $ghg^{-1} \in \mathrm{Ker}(f)$.
Donc $\mathrm{Ker}(f)$ est distingué dans G.

XIII.5.14 Nature d'une suite

[Enoncé]

XIII.5.15 Une relation utile sur les morphismes de groupes

[Enoncé]
On admet que la relation sur G suivante est une relation d'équivalence sur G.

$$\forall g_1, g_2 \in G, g_1 \sim g_2 \Leftrightarrow g_1^{-1} g_2 \in \mathrm{Ker}(f)$$

Ces classes d'équivalence sont les $g\mathrm{Ker}(f) = \{gk, k \in \mathrm{Ker}(f)\}$ pour $g \in G$.
Montrons que $|g\mathrm{Ker}(f)| = |\mathrm{Ker}(f)|$
On pose $\varphi : \left\{ \begin{array}{ccc} \mathrm{Ker}(f) & \longrightarrow & g\mathrm{Ker}(f) \\ k & \longmapsto & gk \end{array} \right.$ et $\psi : \left\{ \begin{array}{ccc} g\mathrm{Ker}(f) & \longrightarrow & \mathrm{Ker}(f) \\ k & \longmapsto & g^{-1}k \end{array} \right.$.
On remarque que : $\varphi \circ \psi = Id_G = \psi \circ \varphi$ donc φ est une bijection et $|g\mathrm{Ker}(f)| = |\mathrm{Ker}(f)|$.
De plus, on remarque que f est constante sur les classes d'équivalence définies précédemment.
En effet, pour tout $g_1, g_2 \in G$ tel que $g_1 \sim g_2$, on a $f(g_1^{-1} g_2) = e$ donc $f(g_1) = f(g_2)$ car f est un morphisme de groupe.
Ainsi, on en déduit que le nombre de classes d'équivalences est $|\mathrm{Im}(f)|$.
Finalement, puisque les classes d'équivalences forment une partition de G, on en déduit :

$$|G| = \sum_{g \in \mathrm{Im}(f)} |g\mathrm{Ker}(f)| = \sum_{g \in \mathrm{Im}(f)} |\mathrm{Ker}(g)| = |\mathrm{Ker}(f)||\mathrm{Im}(f)|$$

XIII.5.16 Automorphisme d'inversion ★

[Enoncé]
Notons e le neutre de G. Soit $x \in G$ tel que $f(x) = e$. Alors $x^{-1} = e$ c'est à dire $e = x$.
$\forall (x, y) \in G^2,\ f(xy) = (xy)^{-1} = y^{-1}x^{-1}$.
Donc $f \in \mathrm{Aut}(G) \iff \forall (x, y) \in G^2,\ y^{-1}x^{-1} = f(xy) = f(x)f(y) = x^{-1}y^{-1} \iff \forall (x, y) \in G^2,\ (y^{-1}x^{-1})^{-1} = (x^{-1}y^{-1})^{-1} \iff \forall (x, y) \in G^2,\ xy = yx$.

XIII.5.17 Automorphismes intérieurs ★

[Enoncé]

1. Notons e le neutre de G. Soient $x, y \in G$.
   $\varphi_a(xy) = axya^{-1} = (axa^{-1})(aya^{-1}) = \varphi_a(x)\varphi_a(y)$.
   $\forall x \in G,\ \varphi_a(x) = e \implies axa^{-1} = e \iff ax = a \implies x = e$.
   Donc $\varphi_a \in \mathrm{Aut}(G)$.
2. Montrons que $\Phi : \left\{ \begin{array}{ccc} (G, *) & \longrightarrow & (\mathrm{Aut}(G), \circ) \\ a & \longmapsto & \varphi_a \end{array} \right.$ est un morphisme de groupes.
   Soient $a, b \in G$. Fixons $x \in G$.
   $\Phi(ab)(x) = abx(ab)^{-1} = a(bxb^{-1})a^{-1} = a\Phi(b)(x)a^{-1} = \Phi(a) \circ \Phi(b)(x)$.
   Donc $\Phi(ab) = \Phi(a) \circ \Phi(b)$.
   Ainsi $\mathfrak{J}(G) = \mathrm{Im}(\Phi)$ est un sous-groupe de $(\mathrm{Aut}(G), \circ)$.

XIII.5.18 Endomorphismes continus de $\mathbb{R}$ ★★

[Enoncé]
Soit f un endomorphisme de $(\mathbb{R},+)$ continu.
Par récurrence immédiate, $\forall n\in\mathbb{N},\ f(n)=nf(1)$. Donc $\forall n\in\mathbb{N},\ f(-n)=-nf(1)$.
Ainsi $\forall k\in\mathbb{Z},\ f(k)=kf(1)$.
Soit $x=\dfrac{a}{b}\in\mathbb{Q}$ avec $a\in\mathbb{Z}$ et $b\in\mathbb{N}^*$.
$bf(x)=f(bx)=f(a)=af(1)$. Donc $f(x)=\dfrac{a}{b}f(1)=xf(1)$.
Les applications f et $x\mapsto f(1)x$ coïncident sur $\mathbb{Q}$. Or $\mathbb{Q}$ est dense dans $\mathbb{R}$ et f est continu sur $\mathbb{R}$ donc f et $x\mapsto f(1)x$ coïncident sur $\mathbb{R}$.
Autrement dit f est l'homothétie de rapport $f(1)$.
Réciproquement on vérifie que les homothéties sont des endomorphismes de $(\mathbb{R},+)$ continus.

XIII.5.19 Morphismes de $\mathbb{Q}$ dans $\mathbb{Z}$ ★

[Enoncé]
Soit f un morphisme de $(\mathbb{Q},+)$ dans $(\mathbb{Z},+)$.
Par récurrence immédiate, $\forall n\in\mathbb{N},\ f(n)=nf(1)$. Fixons $p\in\mathbb{N}$.
$\forall q\in\mathbb{N}^*,\ qf\left(\dfrac{p}{q}\right)=f(p)$ donc $f\left(\dfrac{p}{q}\right)=\dfrac{f(p)}{q}\in\mathbb{Z}$.
Autrement dit $\forall q\in\mathbb{N}^*,\ q|f(p)$. Donc $f(p)=0$.
Ainsi $f=0$.

XIII.5.20 Morphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$

[Enoncé]
On note $\overline{k}$ les éléments de $\mathbb{Z}/n\mathbb{Z}$ et $\tilde{k}$ les éléments de $\mathbb{Z}/m\mathbb{Z}$.
On raisonne par analyse-synthèse.
Soit $f:\mathbb{Z}/n\mathbb{Z}\longrightarrow\mathbb{Z}/m\mathbb{Z}$. Il est clair que pour tout $k\in\mathbb{Z}$,

$$f(\overline{k})=f(k\overline{1})=kf(\overline{1})$$

Ainsi, f est entièrement déterminé par $f(\overline{1})$. De plus,

$$f(\overline{n})=\tilde{0}$$

donc $nf(\overline{1})\equiv 0[m]$.
Ainsi si $f:\mathbb{Z}/n\mathbb{Z}\longrightarrow\mathbb{Z}/m\mathbb{Z}$ est un morphisme alors $nf(\overline{1})\equiv 0[m]$.
La réciproque est immédiate.

XIII.5.21 Morphismes de $\mathrm{GL}_n(\mathbb{R})$ dans $\mathbb{Z}/m\mathbb{Z}$ ★★★★★

[Enoncé]
Soit f un morphisme de $(\mathrm{GL}_n(\mathbb{R}),\times)$ dans $(\mathbb{Z}/m\mathbb{Z},+)$. On note $D_i(\lambda)=I_n+(1-\lambda)E^n_{ii}$

pour $i \in [\![1;n]\!]$ et $\lambda \in \mathbb{R}^*$ les matrices de dilatations (où E_{ij}^n représente la matrice carrée de taille n ayant un 1 en position (i,j) et des 0 partout ailleurs). On note $T_{ij}(\lambda) = I_n + \lambda E_{ij}^n$ pour $(i,j) \in [\![1;n]\!]^2, i \neq j$ et $\lambda \in \mathbb{R}$ les matrices de transvections.
On rappelle que multiplier une matrice de $M \in \mathcal{M}_n(\mathbb{R})$ à gauche par $T_{ij}(\lambda)$ revient à effectuer l'opération $L_i \leftarrow L_i + \lambda L_j$ sur les lignes de M, multiplier une matrice de $M \in \mathcal{M}_n(\mathbb{R})$ à droite par $T_{ij}(\lambda)$ revient à effectuer l'opération $C_i \leftarrow C_i + \lambda C_j$ sur les colonnes de M.
Enfin, on peut échanger les lignes L_i et L_j "au signe près" en effectuant à la suite les opérations $L_i \leftarrow L_i + L_j$, $L_j \leftarrow L_j - L_i$, $L_i \leftarrow L_j + L_i$, autrement dit en multipliant à gauche par $T_{ij}(1)T_{ji}(-1)T_{ij}(1)$. La ligne L_i sera transformée en la ligne L_j et la ligne L_j sera transformée en la ligne $-L_i$.
Montrons par récurrence via l'algorithme du pivot de Gauss que pour toute matrice $A \in \mathrm{GL}_n(\mathbb{R})$, il existe $M, N \in \mathrm{GL}_n(\mathbb{R})$ telles que $MAN = D_n(\det A)$ avec M et N des produits de matrice de transvection.
Si $n = 1$, $A = D_1(\det A)$ et il n'y a rien à faire.
Supposons le résultat vraie à un certain rang $n - 1 \geq 1$. Soit $A \in \mathrm{GL}_n(\mathbb{R})$. La première colonne de A étant non nulle, il existe $i \in [\![1;n]\!]$ tel que $a_{i,1} \neq 0$. L'opération $L_1 \leftarrow L_1 + \dfrac{1 - a_{1,1}}{a_{i,1}} L_i$ permet de remplacer le coefficient en position $(1,1)$ par un 1.
Il est ensuite aisé d'annuler les coefficients de la première ligne et de la première colonne (hormis le 1 en position $(1,1)$) avec des opérations sur les lignes et les colonnes :

— Pour tout $j \in [\![2;n]\!]$, l'opération $C_j \leftarrow C_j - a_{1,j}C_1$ annule le coefficient en position $(1,j)$;

— Pour tout $k \in [\![2;n]\!]$, l'opération $L_k \leftarrow L_k - a_{k,1}L_1$ annule le coefficient en position $(k,1)$.

Ainsi par le biais de produits de matrices de transvection :
$$\begin{cases} M_0 = T_{n,1}(-a_{n,1}) \dots T_{k,1}(-a_{k,1}) \dots T_{2,1}(-a_{2,1}) \\ N_0 = T_{2,1}(-a_{2,1}) \dots T_{k,1}(-a_{k,1}) \dots T_{n,1}(-a_{n,1}) \end{cases}$$
On obtient $M_0AN_0 = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & A_0 \end{array}\right)$.
A_0 est inversible puisque $\det(A_0) = \det(M_0AN_0) = \det(M_0)\det(A)\det(N_0) = \det(A) \neq 0$.
En effet, les matrices de transvection ont un déterminant qui vaut 1 car elles sont triangulaires supérieure/inférieure avec des 1 sur leur diagonale. On peut donc appliquer l'hypothèse de récurrence à A_0 : il existe M_1, N_1 des produits de matrices de transvection telles que $M_1A_0N_1 = D_{n-1}(\det A_0)$.
On pose alors $M = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & M_1 \end{array}\right) M_0$ et $N = N_0 \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & N_1 \end{array}\right)$ de sorte que,
$$MAN = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & M_1 \end{array}\right)\left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & A_0 \end{array}\right)\left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & N_1 \end{array}\right) = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & M_1A_0N_1 \end{array}\right) = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & D_{n-1}(\det A) \end{array}\right) =$$
$D_n(\det A)$ et M, N soient des produits de matrices de transvection.
$\left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & M_1 \end{array}\right)$ est bien une matrice de transvection car pour $(i,j) \in [\![1;n-1]\!]^2$ et $\lambda \in \mathbb{R}$ tel

que $M_1 = I_{n-1} + \lambda E_{ij}^{n-1}$, on a $\left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & M_1 \end{array}\right) = I_n + \lambda E_{ij}^n$. De même, $\left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & N_1 \end{array}\right)$ est bien une matrice de transvection.

Remarque : on a en fait montré que $\mathrm{SL}_n(\mathbb{R})$ *est engendré par les matrices de transvection et que* $\mathrm{GL}_n(\mathbb{R})$ *est engendré par les matrices de transvection et les matrices de dilatation.*

Revenons à f. Pour déterminer un morphisme, il suffit de déterminer l'image d'une partie génératrice. Comme $\mathbb{Z}/m\mathbb{Z}$ est d'ordre m, $\forall A \in \mathrm{GL}_n(\mathbb{R}),\ f(A^m) = \overline{m} f(A) = \overline{0}$.
Puisque $T_{ij}(\lambda) = T_{ij}\left(\frac{\lambda}{m}\right)^m$, on a $f(T_{ij}(\lambda) = 0$. On en déduit que pour tout $A \in \mathrm{GL}_n(\mathbb{R}),\ f(A) = f(D_n(\det A)$.
Si m est impair, pour tout $\lambda \in \mathbb{R}^*,\ D_n(\lambda) = D_n\left(\sqrt[m]{\lambda}\right)^m = \overline{0}$ et donc f est le morphisme trivial.
Si m est pair, pour tout $\lambda \in \mathbb{R}_+^*,\ D_n(\lambda) = D_n\left(\sqrt[m]{\lambda}\right)^m$ donc $f(A) = \overline{0}$ pour tout $A \in \mathrm{GL}_n^+(\mathbb{R})$. De plus, si $\lambda \in \mathbb{R}_-^*,\ D_n(\lambda) = D_n(-1)D_n(-\lambda)$ avec $-\lambda > 0$. Ainsi, $\forall A \in \mathrm{GL}_n^-(\mathbb{R}),\ f(A) = f(D_n(-1))$. Or $D_n(-1)^2 = I_n$ donc $f(D_n(-1)) = \overline{0}$ ou $f(D_n(-1)) = \frac{\overline{m}}{2}$.
Finalement, f est soit le morphisme trivial, soit le morphisme valant $\overline{0}$ sur $\mathrm{GL}_n^+(\mathbb{R})$ et $\frac{\overline{m}}{2}$ et $\mathrm{GL}_n^-(\mathbb{R})$.

XIII.5.22 Caractères algébriques de $GL_n(\mathbb{K})$

[Enoncé]

XIII.5.23 Quasi-morphisme ★★★

[Enoncé]

1. Supposons par l'absurde que f s'annule en $x \in G$.
   Alors par inégalité triangulaire, $\forall y \in G,\ |f(y)| = |f(yx^{-1}x) - f(yx^{-1})f(x)| \leq \delta$ ce qui contredit le caractère non bornée de f.
   Ainsi f ne s'annule pas.
2. Comme f n'est pas bornée, on sait qu'il existe $(z_n) \in G^{\mathbb{N}}$ telle que $|f(z_n)| \underset{n\to+\infty}{\longrightarrow} +\infty$.
   Fixons $x \in G$.
   On peut écrire $\forall n \in \mathbb{N},\ \left|\frac{f(xz_n)}{f(z_n)} - f(x)\right| \leq \frac{\delta}{|f(z_n)|}$.
   Par passage à la limite, $f(x) = \lim\limits_{n\to+\infty} \frac{f(xz_n)}{f(z_n)}$.
3. On considère $(z_n)_{n\in\mathbb{N}}$ comme définie précédemment. Fixons $x, y \in G$.
   $|f(y)| = \lim\limits_{n\to+\infty} \frac{|f(yz_n)|}{|f(z_n)|}$. Donc $(|f(yz_n)|)_{n\in\mathbb{N}}$ diverge vers $+\infty$ et on peut écrire comme f

ne s'annule pas :

$$f(xy) = \lim_{n\to+\infty} \frac{f(xyz_n)}{f(z_n)} = \lim_{n\to+\infty} \frac{f(xyz_n)}{f(yz_n)} \cdot \frac{f(yz_n)}{f(z_n)} = f(x)f(y)$$

XIII.5.24 Morphisme de $\mathbb{Z}^{\mathbb{N}}$ presque nul ★★★

[Enoncé]

1. Soit $n \in \mathbb{N}$. $x_n \in \mathbb{Z}$ et $\text{pgcd}(2^n, 3^n) = 1$ donc d'après le théorème de Bézout, $\exists (y_n, z_n) \in \mathbb{Z}^2,\ 2^n y_n + 3^n z_n = x_n$.

2. Soit $s > 0$.
$\Phi((2^n y_n)) = \Phi(y_0, 2y_1, \dots, 2^{s-1}y_{s-1}, 0, 0, \dots) + \Phi(0, \dots, 0, 2^s y_s, 2^{s+1}y_{s+1}, \dots) = 2^s \Phi(0, \dots, 0, y_s, 2y$
Donc $\Phi((2^n y_n))$ est un multiple de 2^s pour tout $s > 0$ d'où $\Phi((2^n y_n)) = 0$.
De manière analogue, $\Phi((3^n z_n)) = 0$ puis $\Phi((x_n)) = 0$.
Finalement $\Phi = 0$.

XIII.5.25 Groupes de matrices

[Enoncé]
Notons E le neutre de G.
Par définition du neutre $E^2 = E$. Ainsi E est une matrice de projection. On sait (ou redémontre aisément) alors que E est semblable, par la matrice de passage P de la base canonique de $\mathbb{K}^n$ à une base adaptée à la décomposition $\mathcal{M}_n(\mathbb{K}) = \ker(E - I_n) \bigoplus \ker(E)$, à $J_r = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right)$.
En particulier l'application $f : \left\{ \begin{array}{ccc} \text{GL}_r(\mathbb{K}) & \longrightarrow & G \\ M & \longmapsto & P^{-1} \left(\begin{array}{c|c} M & 0 \\ \hline 0 & 0 \end{array}\right) P \end{array} \right.$ est un morphisme de groupes injectif.
Ainsi G est isomorphe à $f^{-1}(G)$ qui est un sous-groupe de $\text{GL}_r(\mathbb{K})$.

XIII.5.26 Caractérisation de la finitude d'un groupe par ses sous-groupes ★★★

[Enoncé]
Notons g l'ensemble des sous-groupes de G.
Si G est fini alors $|\mathcal{P}(G)| = 2^{|G|}$. Donc $g \subset \mathcal{P}(G)$ est fini.
Supposons que g est fini.
On écrit $G = \bigcup_{x\in G} < x >$.
Par hypothèse, il existe une sous partie G_0 finie de G telle que $\{< x >,\ x \in G\} = \{< x >$

, $x \in G_0\}$.
De plus, pour tout $x \in G$, $< x >$ est fini. En effet, Si $< x >$ est infini alors les ensembles $< x^{2^n} >$ pour $n \in \mathbb{N}$ sont des sous-groupes de G tous distincts $\left(< x^{2^{n+1}} > \subset < x^{2^n} > \text{ et } x^{2^n} \notin < x^{2^{n+1}} > \right.$ et g n'est pas fini.

Donc $|G| = \left| \bigcup_{x \in G_0} < x > \right| \leq \sum_{x \in G_0} | < x > | < +\infty$.

XIII.5.27 Sous-groupe des éléments d'ordre fini ★★★★

[Enoncé]
Notons H le sous-groupe engendré par les éléments de E. On va montrer que $E = H$. Par définition, $E \subset H$.
Montrons d'abord que tout élément de H s'écrit comme produit d'éléments distincts de G. On remarque que si $x = ab$ avec $a, b \in E$ alors $x = ba'$ avec $a' = b^{-1}ab \in E$ puisque l'ordre de a' est le même que celui de a en tant que conjugué de celui-ci.
Si x s'écrit $g_1 \dots g_n$ avec $g_1, \dots, g_n \in E$ (On peut toujours écrire cette décomposition sans inverse puisque si $x \in E \implies x^{-1} \in E$) et n le nombre minimal d'éléments de E nécessaire pour décomposer x alors, s'il existe $i < j$ tels que $g_i = g_j$, on répète la méthode décrite précédemment pour écrire $x = g_1 \dots g_i g_j g'_{i+1} \dots g'_{j-1} g_{j+1} \dots g_n$ avec $g'_{i+1}, \dots, g'_{j-1} \in E$. Or $g_i g_j = g_i^2 \in E$ et donc on a écrit x comme produit de $n-1$ éléments de E ce qui est absurde.
Notons $r = |H|$. La décomposition d'un élément de H en produit d'élément de E contient toujours au plus r éléments distincts de E. On peut donc majorer le cardinal de H par $\sum_{k=0}^{r} k!$.
Ainsi H est un groupe d'ordre fini, tous ses éléments sont d'ordre fini i.e $H \subset E$.
Finalement $E = H$.

XIII.5.28 Relations d'équivalence naturelles sur les groupes ★

[Enoncé]
Soit $(x, y, z) \in G^3$. On note e le neutre de G.
$x = ex = xe = e^{-1}xe$ donc $x \sim_g x$, $x \sim_d x$ et $x \sim x$.

Si $x \sim y$ alors il existe $h \in H$ tel que $h^{-1}xh = y$. Alors $x = \left(h^{-1}\right)^{-1} yh^{-1}$ avec $h^{-1} \in H$ puisque H est un groupe, d'où $y \sim x$.
Si $x \sim_d y$ alors il existe $h \in H$ tel que $y = xh$. Alors $x = yh^{-1}$ avec $h^{-1} \in H$ d'où $y \sim_d x$.
Si $x \sim_g y$ alors il existe $h \in H$ tel que $y = hx$. Alors $x = h^{-1}y$ avec $h^{-1} \in H$ d'où $y \sim_g x$.

Si $x \sim y \sim z$ alors il existe $h_0, h_1 \in H$ tels que $y = h_0^{-1}xh_0$ et $z = h_1^{-1}yh_1$. Alors $z = h_2^{-1}xh_2$ avec $h_2 = h_0h_1 \in H$ puisque H est un groupe, d'où $x \sim z$.
Si $x \sim_d y \sim_d z$ alors il existe $h_0, h_1 \in H$ tels que $y = xh_0$ et $z = yh_1$. Alors $z = xh_2$ avec $h_2 = h_0h_1 \in H$ d'où $x \sim_d z$

Si $x \sim_g y \sim_g z$ alors il existe $h_0, h_1 \in H$ tels que $y = h_0 x$ et $z = h_1 y$. Alors $z = h_2 x$ avec $h_2 = h_1 h_0 \in H$ d'où $x \sim_g z$
Ainsi $\sim$, $\sim_d$ et $\sim_g$ sont des relations d'équivalence sur G

XIII.5.29 Théorème de Lagrange ★★★

[Enoncé]
Soit H un sous-groupe de G. On note e le neutre de G.
On définit la relation binaire $\sim$ sur G par $x \sim y \iff \exists h \in H,\ x = yh$. $\sim$ est une relation d'équivalence :

- $\forall x \in G,\ x = xe \implies x \sim x$;
- $\forall x, y \in G,\ x \sim y \implies \exists h \in H,\ x = yh \implies \exists h' = h^{-1} \in H,\ y = xh' \implies y \sim x$;
- Si $x, y, z \in G$ tels que $x \sim y$ et $y \sim z$ alors il existe $h, h' \in H$ tels que $x = yh$ et $y = zh'$. Alors $h'' = h'h \in H$ et $x = zh''$ d'où $x \sim z$.

Pour $x \in G$ on note xH la classe d'équivalence de x pour la relation $\sim$. Pour tout $x \in G$, l'application $h \in H \mapsto xh$ est bijective de H sur xH. En effet, elle est clairement surjective et de plus, si $h_1, h_2 \in H$ tels que $xh_1 = xh_2$ alors en multipliant par x^{-1} à gauche on obtient $h_1 = h_2$. Ainsi pour $\forall x \in G,\ |H| = |xH|$.
Notons $x_1, \dots, x_d$ un système de représentant de la relation $\sim$.
$G = \bigsqcup_{k=1}^{d} x_k H$ donc $|G| = \sum_{k=1}^{d} |x_k H| = \sum_{k=1}^{d} |H| = d|H|$.
Ainsi $|H|$ divise $|G|$.

XIII.5.30 Un cas particulier du lemme de Cauchy ★★★★

[Enoncé]

1. a. $\forall x \in G,\ x^2 = e \implies x = x^{-1}$.
   Donc $\forall x, y \in G,\ (xy)^2 = xyxy = e \implies yx = x^{-1}y^{-1} = xy$
   b. Définissons la loi $+$ sur G par $\forall (x, y) \in G^2,\ x + y = x * y$ et la loi $\cdot$ sur $\mathbb{Z}/2\mathbb{Z} \times G$ par :
   - $\forall x \in G,\ \overline{0}x = e$
   - $\forall x \in G,\ \overline{1}x = x$

   Autrement dit $\forall (a, x) \in \{0, 1\} \times G,\ \overline{a} \cdot x = x^a$ ($x^2 = e$ assure que cela reste vrai pour $a \in \mathbb{Z}$). Vérifions que $(G, +, \cdot)$ est un $\mathbb{Z}/2\mathbb{Z}$ espace-vectoriel.
   Tout d'abord $(G, +)$ est un groupe commutatif. Ensuite fixons $a, b \in \{0, 1\}$ ainsi que $x, y \in G$.
   - $(\overline{a} + \overline{b}) \cdot x = \overline{a + b} \cdot x = x^{a+b} = x^a x^b = \overline{a} \cdot x + \overline{b} \cdot x$;
   - $\overline{a} \cdot (x + y) = \overline{a} \cdot (xy) = (xy)^a = x^a y^a = \overline{a} \cdot x + \overline{a} \cdot y$;

— $\overline{a} \cdot (\overline{b} \cdot x) = \overline{a} \cdot x^b = \left(x^b\right)^a = x^{ab} = \overline{ab} \cdot x$;
— $\overline{1}x = x$.

Ainsi $(G, +, \cdot)$ définit bien un espace vectoriel.
Cet espace est fini et donc a fortiori de dimension finie.
Posons $(e_1, \dots, e_p)$ une base de G.

Alors $\varphi : \left\{ \begin{array}{ccc} G & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})^p \\ x = \sum_{i=1}^{p} a_i e_i & \longmapsto & (a_1, \dots, a_p) \end{array} \right.$ est bijective d'où $|G| = 2^p$.

2. Soit $x \in G \backslash \{e\}$. D'après le théorème de Lagrange, l'ordre n de x divise $2p$. Donc comme p est premier, $n = 2$ ou $n = p$ ou $n = 2p$. Si $n = p$ alors il n'y a rien à faire. Si $n = 2p$ alors $y = x^2$ est d'ordre p.
Dans le dernier cas, tous les éléments de $G \backslash \{e\}$ sont d'ordre 2.
Mais alors d'après la question 1 $|G| = 2^q$ pour un certain entier q. Or $p > 2$ apparaît dans la décomposition en facteur premier de $|G|$. Ceci est absurde donc il existe un élément dans G qui n'est pas d'ordre 2.

XIII.5.31 Groupe d'ordre premier ★

[Enoncé]
Il s'agit de montrer que G possède un élément d'ordre p. Soit $x \in G$.
D'après le théorème de Lagrange l'ordre de x divise p. Alors comme p est premier, x est d'ordre 1 ou d'ordre p.
Si tous les éléments de G sont d'ordre 1 alors $G = \{e\}$ n'est pas de cardinal $p \geq 2$.
Ainsi il existe $x \in G$ d'ordre p et donc $G =< x >$.

Plus petit groupe non commutatif

1. Soit G un groupe cyclique. Il existe $x \in G$ tel que $G = \langle x \rangle$. Donc G est a fortiori commutatif.
2. Déjà à partir de l'exercice précédent, nous pouvons éliminer les groupes d'ordre 2, 3 et 5. Et évidemment le groupe trivial est commutatif.
Montrons que l'on peut également éliminer 4.
Soit G un groupe d'ordre 4.
D'après le théorème de Lagrange, l'ordre de tout élément de G divise l'ordre de G ainsi les ordres possibles pour les éléments différents du neutre sont 2 ou 4.
   — Si G contient un élément d'ordre 4. On note cet élément a. Le sous-groupe cyclique engendré par a contient 4 éléments distincts. Ainsi, $\langle a \rangle = G$ Donc G est cyclique donc G est commutatif.
   — Si tous les éléments non neutres de G sont d'ordre 2. D'après l'exercice V.3, G est commutatif.

Finalement, aucun groupe d'ordre 4 n'est non commutatif. Cet entier est 6. Il suffit de regarder le groupe symétriques S_3 qui n'est pas commutatif.

XIII.5.32 Sous-groupe d'un groupe cyclique ★★★

[Enoncé]

Notons e le neutre de G. Posons x un générateur de G puis posons $y = x^{n/d}$.

Par définition x est d'ordre n donc $y^d = x^n = e$ et $\forall k \in [\![1; d-1]\!],\ \dfrac{nk}{d} < n \implies y^k = x^{nk/d} \neq e$. Ainsi y est d'ordre d d'où $< y >$ est un sous-groupe (cyclique) de G d'ordre d.

Soit H un sous-groupe de G d'ordre d. Fixons $z \in H$.

Comme $z \in G,\ \exists k \in [\![1; n]\!],\ z = x^k$.

De plus $z \in H$ donc $z^d = x^{kd} = e$. Alors d'après le théorème de Lagrange $n|kd$ c'est à dire $\dfrac{n}{d}|k$.

Ainsi $\exists q \in \mathbb{Z},\ k = q \cdot \dfrac{n}{d}$. On a alors $z = x^{q \cdot n/d} = y^q : z \in < y >$.

Finalement $H \subset < y >$ et comme $|H| = d = | < y > |,\ H = < y >$.

XIII.5.33 Exposant d'un groupe abélien fini ★★★★

[Enoncé]

1. $(xy)^{O(x)O(y)} = \left(x^{O(x)}\right)^{O(y)} \cdot \left(y^{O(y)}\right)^{O(x)} = e$ donc $O(xy)|O(x)O(y)$. De plus $(xy)^{O(xy)} = x^{O(xy)}y^{O(xy)} \implies x^{O(xy)} = y^{-O(xy)}$.
   Donc en passant à l'exposant $O(y)$, $x^{O(xy)O(y)} = e$ d'où $O(x)|O(xy)O(y)$.
   Or $O(x) \wedge O(y) = 1$ donc d'après le lemme de Gauss, $O(x)|O(xy)$.
   De même, $O(y)|O(xy)$ puis comme $O(x) \wedge O(y) = 1,\ O(x)O(y)|O(xy)$.
   Finalement $O(xy) = O(x)O(y)$.
   Dans le cas général on a pas $O(xy) = \text{ppcm}(O(x), O(y))$. Par exemple pour $x = y^{-1}$ avec $x \neq e$, $xy = e$ est d'ordre 1 alors que $\text{ppcm}(O(x), O(y)) = \text{ppcm}(O(x), O(x)) = O(x) \neq 1$.
2. Pour que $m'|m$ et $n'|n$ il faut et il suffit que pour tout p premier $v_p(m') \leq v_p(m)$ et $v_p(n') \leq v_p(n)$. Pour que m' et n' soit premier entre eux il faut et il suffit que pour tout p premier $v_p(n') = 0$ ou $v_p(m') = 0$. Enfin pour que $\text{ppcm}(m, n) = m'n'$ il faut et il suffit que pour tout p premier $\max(v_p(m), v_p(n)) = v_p(m') + v_p(n')$.
   On pose donc naturellement $m' = \prod_{p \text{ premier}} p^{\alpha_p}$ et $n = \prod_{p \text{ premier}} p^{\beta_p}$ avec :
   $$\begin{cases} \alpha_p = v_p(m) & \text{si } v_p(m) \geq v_p(n) \\ \alpha_p = 0 & \text{sinon} \end{cases} \text{ et } \begin{cases} \beta_p = v_p(n) & \text{si } v_p(n) > v_p(m) \\ \beta_p = 0 & \text{sinon} \end{cases}$$
3. Notons $G = \{x_1, \ldots, x_n\}$. Montrons par récurrence que pour tout $k \in [\![1; n]\!],\ \exists z_k \in G,\ O(z_k) = \text{ppcm}(O(x_1), \ldots, O(x_k))$.
   Pour $k = 1,\ z_1 = x_1 \in G$ et $O(z_1) = O(x_1)$.
   Supposons le résultat vrai pour un certain $k \in [\![1; n-1]\!]$.

D'après la question précédente, il existe $m', n' \in \mathbb{N}^*$ tels que $m'|O(z_k),\ n'|O(x_{k+1}),\ \text{pgcd}(m', n') = 1,\ m'n' = \text{ppcm}(O(z_k), O(x_{k+1}))$.
Alors $z_k^{O(z_k)/m'}$ et $x_{k+1}^{O(x_{k+1})/n'}$ sont d'ordres m' et n' respectivement, et d'après la question 1,
pour $z_{k+1} = z_k^{O(z_k)/m'} x_{k+1}^{O(x_{k+1})/n'} \in G,\ O(z_{k+1}) = m'n' = \text{ppcm}(O(x_1), \dots, O(x_{k+1}))$.
Par conséquent la propriété est vrai en particulier au rang n ce qui répond à la question.

4. Notons $n = |G|$. G est cyclique si et seulement s'il existe un élément de G d'ordre n, si et seulement si G est d'exposant n. Notons m l'exposant de G.
$\forall x \in G,\ x^m = 1$. C'est à dire $\forall x \in G,\ x^m - 1 = 0$. Le polynôme $X^m - 1$ a donc au moins n racines dans $\mathbb{K}$. Or ce polynôme à au plus m racines dans $\mathbb{K}$. Ainsi $n \leq m$.
Or d'après la question précédente il existe un élément de G d'ordre m. Donc $m \leq n$.
On en déduit que $m = n$ et donc que G est cyclique.

Remarque : une conséquence de la question 4 est le fait que $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique.

XIII.5.34 Un groupe d'inversible non cyclique

[Enoncé]

XIII.5.35 Ordre dans un groupe de cardinal pair

[Enoncé]

1. Réflexivité : Trivial, pour tout $x \in G, x = x$
Symétrie : Par symétrie de l'égalité et par unicité de l'inverse, pour tout $x, y \in G, x = y \Rightarrow y = x$ et $x = y^{-1} \Rightarrow y = x^{-1}$
Transitivité : Soit x, y, z tel que $x\mathcal{R}y$ et $y\mathcal{R}z$.
   — Si $x = y$ alors on a immédiatement $x\mathcal{R}z$.
   — Si $x = y^{-1}$, on sait que : $y = z$ ou $y = z^{-1}$ donc $x^{-1} = z$ ou $x^{-1} = z^{-1}$. D'où le résultat.

   Ainsi cette relation $\mathcal{R}$ sur G est une relation d'équivalence sur G.
2. On remarque que les classes d'équivalence sont de la forme : $\text{cl}(x) = \{x, x^{-1}\}$ pour tout $x \in G$. On remarque également que $\text{cl}(e) = \{e\}$. Ainsi chaque classe d'équivalence contient 1 ou 2 éléments. Et puisque $\text{cl}(e)$ contient un unique élément et que le cardinal de G est pair, il existe une autre classe $\text{cl}(x)$ avec $x \neq e$ de cardinal 1.
Ainsi $x = x^{-1}$ cad $x^2 = e$. Par conséquent, G admet un élément d'ordre deux.

XIII.5.36 Ordre dans $\mathbb{Z}/n\mathbb{Z}$ ★★

[Enoncé]

D'une part, $\dfrac{k}{k \wedge n} \in \mathbb{N} \implies \dfrac{n}{n \wedge k}\overline{k} = \dfrac{k}{n \wedge k}\overline{n} = \overline{0}$. Donc $d|\dfrac{n}{n \wedge k}$.

D'autre part, $\overline{dk} = d\overline{k} = \overline{0}$ donc $n|dk$.
Alors $\frac{n}{n \wedge k} | d \cdot \frac{k}{n \wedge k}$. Or pgcd $\left(\frac{n}{n \wedge k}, \frac{k}{n \wedge k} \right) = 1$ donc d'après le lemme de Gauss, $\frac{n}{n \wedge k} | d$.
Ainsi comme $d \geq 0$ et $\frac{n}{n \wedge k} \geq 0$, $d = \frac{n}{n \wedge k}$.

XIII.5.37 Passage par les groupes

[Enoncé]

1. On peut déjà éliminer le cas où n=2, car $2 \nmid 3$. On sait que $2 \wedge p = 1$ donc $2^{p-1} \equiv 1[p]$ d'après le lemme de Fermat.
   Donc $m|p-1$.
2. On a supposé que $n|2^n - 1$. Donc $2^n \equiv 1[n]$. Et puisque $p|n$, $2^n \equiv 1[p]$. Donc $m|n$.
3. Puisque p est le plus petit diviseur premier de n et que $m|n$ on n'en déduit que tous les facteurs premiers de m sont supérieurs ou égals à p. Donc $m \geq p$
   Mais puisque $m|p-1$, cela signifie que $m < p$.
   On obtient donc une absurdité. Ainsi il n'existe pas de $n \geq 2$ tel que $n|2^n - 1$.

XIII.5.38 Groupe infini non monogène ★

[Enoncé]
$(\mathbb{Z}^2, +)$ n'est pas monogène.
$\forall (a,b) \in \mathbb{Z}^2, \ < (a,b) >= \{(ka, kb), \ k \in \mathbb{Z}\} \neq \mathbb{Z}^2$.

XIII.5.39 Groupe non cyclique ★★

[Enoncé]
Si $m \wedge n = 1$ alors d'après le théorème des restes chinois on sait que $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est isomorphe à $\mathbb{Z}/mn\mathbb{Z}$ en tant qu'anneau. Donc $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +)$ est isomorphe à $(\mathbb{Z}/mn\mathbb{Z}, +)$ d'où $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +)$ est cyclique.
Réciproquement supposons que $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +)$ est cyclique. Posons (a,b) un générateur.
On notera $\overline{k}$ et $\tilde{k}$ les classes respectives d'un entier k dans $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$.
Comme $m \vee n$ est un multiple de m et de n, $(m \vee n)a = \overline{0}$ et $(m \vee n)b = \tilde{0}$. Donc l'ordre de (a,b), qui vaut mn en tant que générateur, divise $m \vee n$.
Or $m \wedge n \times m \vee n = mn$. Donc $m \wedge n$ divise 1 c'est à dire $m \wedge n = 1$.

XIII.5.40 Ordre dans le groupe symétrique ★

[Enoncé]
Soient $n \in \mathbb{N}^*$ et $\sigma \in \mathcal{S}_n$.

On note $\sigma = \prod_{i=1}^{p} c_i$ la décomposition de σ en produit de cycles à supports disjoints.

On sait que deux cycles à supports disjoints commutent. Donc $\forall k \in \mathbb{N}^*,\ \sigma^k = \prod_{i=1}^{p} c_i^k$.

Notons pour $1 \leq i \leq p,\ m_i$ l'ordre de c_i et posons $m = \text{ppcm}(m_1, \dots, m_p)$. par unicité de la décomposition en produit de cycles à supports disjoints :

$$\begin{aligned} &\forall k \in \mathbb{N}^*,\ \sigma^k = \text{Id} \\ &\iff \forall i \in [\![1; p]\!],\ c_i^k = \text{Id} \\ &\iff \forall i \in [\![1; p]\!],\ m_i | k \\ &\iff m | k \end{aligned}$$

Ainsi σ est d'ordre m.

XIII.5.41 Sous-groupe engendré par les nombres premiers

[Enoncé]

On a :

$$\langle \mathcal{P} \rangle = \left\{ \prod_{i=1}^{r} p_i^{k_i}, r \in \mathbb{N}, \forall i \in [\![1; r]\!], p_i \in \mathcal{P}, k_i \in \mathbb{Z} \right\}$$

Il est clair que :

$$\langle \mathcal{P} \rangle \subset \mathbb{Q}^*$$

Soit $q = \frac{a}{b}$.
D'après la décomposition en facteurs premiers de a et b, on en déduit que $q \in \langle \mathcal{P} \rangle$.
Par conséquent,

$$\langle \mathcal{P} \rangle = \mathbb{Q}^*$$

XIII.5.42 Sous-groupe engendré par le complémentaire d'un sous-groupe

[Enoncé]

XIII.5.43 Partie génératrice

[Enoncé]

XIII.5.44 Groupe alterné ★★★

[Enoncé]

1. L'application signature $\varepsilon : \mathcal{S}_n \to \{-1, 1\}$ est un morphisme de groupes donc $\mathcal{A}_n = \ker \varepsilon$ est un sous-groupe de $\mathcal{S}_n$.
2. On sait que tout élément de $\mathcal{S}_n$ peut s'écrire comme composition de transpositions. La signature d'une transposition valant -1, tout élément de $\mathcal{A}_n$ s'écrit comme composition d'un nombre pair de transpositions. Quitte à rassembler ces transpositions deux par deux, il suffit de montrer que la composée de 2 transposition peut toujours s'écrire comme une composition de 3-cycle :
   Soient τ_1, τ_2 deux transpositions :
   Si $\tau_1 = \tau_2$, $\tau_1 \circ \tau_2 = \mathrm{Id} = (1,2,3) \circ (2,3,1)$;
   Si $\tau_1 = (i,j)$, et $\tau_2 = (j,k)$ avec i,j,k distincts alors $\tau_1 \circ \tau_2 = (i,j,k)$;
   Si $\tau_1 = (i,j)$, et $\tau_2 = (k,l)$ avec i,j,k,l distincts alors $\tau_1 \circ \tau_2 = (i,j,k) \circ (j,k,l)$.

XIII.5.45 Cardinal minimal d'une famille de transpositions engendrant $\mathcal{S}_n$

[Enoncé]

1. On rappelle que $\mathcal{S}_n$ est engendré par les transpositions.
   Ainsi, il suffit de montrer que toutes transpositions se décompose dans $(t_2, \dots, t_n)$.
   Soit $(i,j) \in [\![1;n]\!]^2$
   $$(i\,j) = (1\,i)(1\,j)(1\,i)$$
   Donc $\{t_2, \dots, t_n\}$ engendre $\mathcal{S}_n$.
2. Pour la transposition $s = (i\,j)$, géométriquement, cela revient à dire que u est une réflexion orthogonale d'hyperplan
   $$H = \{x \in \mathbb{R}^n, x_i = x_j\}$$
3. *Première méthode* : Si s est le produit de p transpositions alors $\mathrm{Ker}(u_s - Id_E)$ contient l'intersection des p hyperplans associées à chacune des transpositions.
   Or, on remarque que $\mathrm{Ker}(u_s - Id_E) = \mathrm{Vect}(e_1 + \dots + e_n) = 1$ d'où le résultat.
   Deuxième méthode :On observe que lorsque l'on multiplie une permutation σ par une transposition, cela revient à rassembler deux cycles ou au contraire à couper en 2 un cycle.
   Ainsi, en partant de l'identité qui a n cycles, on en déduit que s a au moins $n-p$ cycles d'après ce qui précède. Ainsi, puisque s est un n-cycle, il a un unique cycle, donc on en déduit que $n - p \leq 1$, d'où $p \geq n-1$.
4. D'après ce qui précède, on en déduit que $n-1$ est ce minimum.

XIII.5.46 Partie génératrice de $\mathcal{O}(E)$

[Enoncé]

XIII.5.47 Groupe dans un plan euclidien

[Enoncé]

XIII.5.48 Matrices de permutation ★

[Enoncé]

1. Soit $(\sigma,\tau)\in\mathfrak{S}_n^2$. Fixons $(i,j)\in[\![1;n]\!]^2$.
   $(f(\sigma)f(\tau))_{i,j}=\sum_{k=1}^{n}f(\sigma)_{i,k}f(\tau)_{k,j}=\sum_{k=1}^{n}\delta_{i,\sigma(k)}\delta_{k,\tau(j)}=\delta_{\sigma^{-1}(i),\tau(j)}$.
   Or $\sigma^{-1}(i)=\tau(j)\iff i=\sigma\circ\tau(j)$. Donc $\delta_{\sigma^{-1}(i),\tau(j)}=\delta_{i,\sigma\circ\tau(j)}$.
   Ainsi $f(\sigma)f(\tau)=P_{\sigma\circ\tau}=f(\sigma\circ\tau)$.
   Donc f est un morphisme et on en déduit que $\mathcal{P}_n=\mathrm{Im}(f)$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.
   De plus, $\forall\sigma\in\mathfrak{S}_n,\ f(\sigma)=I_n\implies\forall i\in[\![1;n]\!],\ \delta_{i,\sigma(i)}=1\implies\forall i\in[\![1;n]\!],\ \sigma(i)=i\implies\sigma=\mathrm{Id}$. Donc f est un isomorphisme de groupes.
2. $\forall\sigma\in\mathfrak{S}_n,\ \forall(i,j)\in[\![1;n]\!]^2,\ (P_\sigma^\top)_{i,j}=\delta_{j,\sigma(i)}=\delta_{\sigma^{-1}(j),i}=(P_{\sigma^{-1}})_{i,j}=(P_\sigma^{-1})_{i,j}$.
   Donc $\forall\sigma\in\mathfrak{S}_n,\ P_\sigma^\top=P_\sigma^{-1}$.
   On a montré que $\mathcal{P}_n\subset\mathcal{O}_n(\mathbb{R})$.
3. Soit $\sigma\in\mathfrak{S}_n$.
   Par la formule du déterminant : On sait que $\det(P_\sigma)=\sum_{\tau\in\mathfrak{S}_n}\varepsilon(\tau)\prod_{i=1}^{n}(P_\sigma)_{i,\tau(i)}=\sum_{\tau\in\mathfrak{S}_n}\varepsilon(\tau)\prod_{i=1}^{n}\delta_{i,\sigma\circ\tau(i)}$
   Or $\tau\neq\sigma^{-1}\implies\exists i\in[\![1;n]\!],\ i\neq\sigma\circ\tau(i)\implies\prod_{i=1}^{n}\delta_{i\sigma\circ\tau(i)}=0$ et, $\tau=\sigma^{-1}\implies\forall i\in[\![1;n]\!],\ i=\sigma\circ\tau(i)\implies\prod_{i=1}^{n}\delta_{i\sigma\circ\tau(i)}=1$.
   Finalement $\det(P_\sigma)=\varepsilon(\sigma^{-1})=\varepsilon(\sigma)^{-1}=\varepsilon(\sigma)$.
   Par la définition de la signature :
   On rappelle que dans le programme de MPSI l'application signature est définie comme l'unique morphisme de groupes de S_n dans $\{-1,1\}$ qui vaut -1 sur les transpositions.
   $\det\circ f=\sigma\mapsto\det(P_\sigma)$ est bien un morphisme de groupes de S_n dans $\{-1,1\}$.
   Fixons une transposition $\tau=(i,j)\in\mathfrak{S}_n$ (avec $i<j$). En notant $(E_1,\dots,E_n)$ la base

canonique de $\mathcal{M}_{n,1}(\mathbb{R})$ on a :

$$\begin{aligned}\det(P_\tau) &= \det\left(\ E_1 \mid \dots \mid E_{i-1} \mid E_j \mid E_{i+1} \mid \dots \mid E_{j-1} \mid E_i \mid E_{j+1} \mid \dots \mid E_n\ \right)\\ &\underset{E_i \longleftrightarrow E_j}{=} -\det\left(\ E_1 \mid \dots \mid E_{i-1} \mid E_i \mid E_{i+1} \mid \dots \mid E_{j-1} \mid E_j \mid E_{j+1} \mid \dots \mid E_n\ \right)\\ &= -\det(I_n)\\ &= -1\end{aligned}$$

D'où $\det(P_\sigma) = \varepsilon(\sigma)$. *Remarque* : On peut simplement regarder le déterminant des colonnes et remarquer que les colonnes de P_σ correspond à la permutation σ des colonnes de I_n d'où le résultat car det est alterné.

XIII.5.49 Groupe dérivé ★★★★★

[Enoncé]

1. Notons pour $(x,y) \in G^2$, $[x,y] = xyx^{-1}y^{-1}$. Fixons $(x,y) \in G^2$
   $[x,y]^2 = (xyx^{-1}y^{-1})(xyx^{-1}y^{-1}) = x^2(x^{-1}y)^2(y^{-1})^2$ donc $[x,y] \in C$.
   Ainsi $D \subset C$.
2. Soit $x \in G$. $\exists x_1, \dots, x_n \in G,\ x = x_1 \dots x_n \wedge \forall k \in [\![1;n]\!],\ x_k = x_k^{-1}$.
   On montre par récurrence que pour tout $i \in [\![2;n]\!],\ x_i^{-1} \dots x_2^{-1} = (x_2 \dots x_i)^{-1}$:
   Pour $i = 2$, $x_2 = x_2^{-1}$. Si le résultat est vraie pour un certain $i \in [\![2;n-1]\!]$ alors,
   $(x_2 \dots x_{i+1})^{-1} = x_{i+1}^{-1}(x_2 \dots x_i)^{-1} = x_{i+1}^{-1} \dots x_2^{-1}$.
   Ainsi, $x^2 = (x_1 \dots x_n)(x_1 \dots x_n) = x_1(x_2 \dots x_n)x_1^{-1}(x_2 \dots x_n)^{-1}(x_2 \dots x_n)^2 = [x_1, x_2 \dots x_n](x_2 \dots x$
   On va donc raisonner par récurrence sur n :
   $n = 1 : x^2 = x_1^2 \in D$.
   $n = 2 : x^2 = x_1x_2x_1x_2 = x_1x_2x_1^{-1}x_2^{-1} = [x_1, x_2] \in D$.
   Fixons $n \geq 1$ et supposons que le produit de $n-1$ involutions ($y^{-1} = y$) de G est dans D.
   Alors $x^2 = [x_1, x_2 \dots x_n](x_2 \dots x_n)^2 \in D$ comme produit de deux éléments de D.
   Ainsi $C \subset D$ d'où $D = C$.
3. a. Soit $M = \begin{pmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{pmatrix} \in \mathrm{SO}_2(\mathbb{R})$. Soient $A = \begin{pmatrix}\cos(\alpha) & \sin(\alpha)\\ \sin(\alpha) & -\cos(\alpha)\end{pmatrix}$ et $B = \begin{pmatrix}\cos(\beta) & \sin(\beta)\\ \sin(\beta) & -\cos(\beta)\end{pmatrix}$ deux réflexions.

$$M = AB \iff \begin{cases}\cos(\theta) = \cos(\alpha-\beta)\\ \sin(\theta) = \sin(\alpha-\beta)\\ -\sin(\theta) = \sin(\beta-\alpha)\\ \cos(\theta) = \cos(\alpha-\beta)\end{cases} \iff \theta \equiv \alpha - \beta [2\pi].$$

   Il y a donc existence mais pas unicité de l'écriture de M comme produit de deux symétries.

b. $\mathrm{SO}_2(\mathbb{Q}) \subset \mathrm{SO}_2(\mathbb{R})$ qui est un groupe abélien donc les éléments de $\mathrm{SO}_2(\mathbb{Q})$ commutent tous entre eux. $I_2 \in \mathcal{O}_2(\mathbb{Q})$. De plus, $\det(\mathcal{O}_2(\mathbb{Q})) \subset \det(\mathcal{O}_2(\mathbb{R})) = \{-1, 1\}$. Donc si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $M' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ sont dans $\mathcal{O}_2(\mathbb{Q})$ alors en notant $\varepsilon = \dfrac{1}{\det(M(M')^{-1})} \in \{-1, 1\}$,
$M(M')^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \varepsilon \begin{pmatrix} d' & -b' \\ -c' & d' \end{pmatrix} = \varepsilon \begin{pmatrix} ad' - bc' & bd' - ab' \\ cd' - dc' & dd' - db' \end{pmatrix} \in \mathcal{M}_2(\mathbb{Q})$ d'où $M(M')^{-1} \in \mathcal{O}_2(\mathbb{Q})$. De plus, si $\det(M) = \det(M') = 1$ alors $\det(M(M')^{-1}) = 1$ donc $\mathrm{SO}_2(\mathbb{Q})$ est un sous groupe de $\mathcal{O}_2(\mathbb{Q})$.
Il est évident que $D \subset \mathrm{SO}_2(\mathbb{Q})$. Supposons par l'absurde que $D = C = \mathrm{SO}_2(\mathbb{Q})$. Comme tous les éléments de $\mathcal{O}_2(\mathbb{Q}) \backslash \mathrm{SO}_2(\mathbb{Q})$ ont un carré égal au neutre, C est engendré par les carrés des éléments de $\mathrm{SO}_2(\mathbb{Q})$.
Ensuite, les éléments de $\mathcal{O}_2(\mathbb{Q})$ de déterminant -1 sont des réflexions.
Soit $M \in \mathrm{SO}_2(\mathbb{Q})$. D'après les calculs fait en question 3.*a*, en prenant $\alpha = \theta$ et $\beta = 0$ on a $M = AB$ avec $A = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix} \in \mathcal{O}_2(\mathbb{Q})$, $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathcal{O}_2(\mathbb{Q})$, $A^2 = B^2 = I_2$.
Ainsi $\mathcal{O}_2(\mathbb{Q})$ est bien engendré par les involutions d'où $D = C$ d'après la question 2.
Or comme $\mathrm{SO}_2(\mathbb{Q})$ est commutatif, un produit de carré de matrices de $\mathrm{SO}_2(\mathbb{Q})$ est encore un carré dans $\mathrm{SO}_2(\mathbb{Q})$.
Et donc pour montrer que D est distinct de $\mathrm{SO}_2(\mathbb{Q})$ il suffit de montrer qu'il existe une matrice de $\mathrm{SO}_2(\mathbb{Q})$ qui n'est pas un carré dans $\mathrm{SO}_2(\mathbb{Q})$. C'est le cas de $M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Supposons qu'il existe une matrice $N \in \mathcal{O}_2(\mathbb{Q})$ telle que $M = N^2$.
On a forcément $N \in \mathrm{SO}_2(\mathbb{Q})$ puisque sinon $N^2 = I_n$. On peut donc écrire $N = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$ avec $\theta \in \mathbb{R}$. Mais alors $2\theta \equiv \dfrac{\pi}{2}[2\pi]$ et donc $\cos(\theta) = \pm\dfrac{\sqrt{2}}{2} \notin \mathbb{Q}$ ce qui est absurde.

XIII.5.50 Sous-groupe discret de $\mathbb{C}$ et de $\mathrm{SL}_2(\mathbb{R})$ ★★★★★

[Enoncé]

1. l'ensemble des entiers relatifs $\mathbb{Z}$ et l'ensemble des entiers de Gauss $\mathbb{Z}[i] = \{a + bi,\ (a, b) \in \mathbb{Z}^2\}$ sont des sous-groupes discret de $\mathbb{C}$. $\mathrm{SL}_2(\mathbb{Z})$ en est un de $\mathrm{SL}_2(\mathbb{R})$.

   Remarque : Plus précisément, $\mathbb{Z}[i]$ est un réseau de $\mathbb{C}$. C'est à dire qu'en plus d'être un sous-groupe discret, il engendre $\mathbb{C} \simeq \mathbb{R}^2$ en tant qu'espace vectoriel réel. A contrario $\mathbb{Z}$ n'est pas un réseau de $\mathbb{C}$, mais est un réseau de $\mathbb{R}$. L'étude des réseaux à des applications dans de multiples branches des mathématiques comme la théorie des groupes la géométrie convexe ou la géométrie des nombres. De manière plus pragmatique les réseaux apparaissent dans des problèmes de pavage du plan ou en cristallographie

2. Γ n'étant pas réduit à $\{0\}$ on peut considérer un élément $\gamma \in \Gamma\backslash\{0\}$ de module minimal. Par hypothèse $\exists \gamma' \in \Gamma,\ \gamma = \lambda\gamma'$. De plus $\gamma' \neq 0$ puisque $\mathbb{C}$ est intègre et $\gamma \neq 0$. On a $|\gamma| = |\lambda||\gamma'| \geq |\lambda||\gamma|$ donc $|\lambda| \leq 1$. Or si $|\lambda| < 1$ alors $(\lambda^n\gamma)_{n\in\mathbb{N}}$ est une suite de Γ qui converge vers $0 \in \Gamma$. Dans ce cas 0 n'est pas un point isolé de Γ ce qui est absurde. On en déduit que $|\lambda| = 1$. Notons $\lambda = e^{i\theta}$ avec $\theta \in \mathbb{R}$.
On remarque que $\dfrac{1}{\lambda}\gamma = \gamma' \in \Gamma$. Donc $\lambda\gamma + \dfrac{1}{\lambda}\gamma = 2\cos(\theta)\gamma = (e^{i\theta} + e^{-i\theta})\gamma = 2\cos(\theta)\gamma \in \Gamma$.
Comme Γ est un sous-groupe additif, $\{2\cos(\theta)\}\gamma \in \Gamma$ en notant $\{2\cos(\theta)\} = 2\cos(\theta) - \lfloor 2\cos(\theta)\rfloor \in [0, 1[$.
Si $\{2\cos(\theta)\} \neq 0$ alors en passant au module $\{2\cos(\theta)\} \geq 1$ ce qui est absurde. Donc $\{2\cos(\theta)\} = 0$ i.e $2\cos(\theta) \in \mathbb{Z}$. De plus $2\cos(\theta) \in [-2, 2]$ donc $\cos(\theta) \in \left\{-1, -\dfrac{1}{2}, 0, \dfrac{1}{2}, 1\right\}$.
Si $\cos(\theta) \in \{-1, 0, 1\}$ alors $\lambda^4 = 1$ et si $\cos(\theta) \in \left\{-\dfrac{1}{2}, \dfrac{1}{2}\right\}$ alors $\lambda^6 = 1$.

3. Notons $M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $D = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$. On montre classiquement que $\forall k \in \mathbb{Z},\ M^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$.
Donc $\forall m, n \in \mathbb{Z},\ M^n D^m = \begin{pmatrix} \lambda^m & n\lambda^{-m} \\ 0 & \lambda^{-m} \end{pmatrix}$ et $D^m M^n = \begin{pmatrix} \lambda^m & n\lambda^m \\ 0 & \lambda^{-m} \end{pmatrix}$.

XIII.6 Correction Anneaux et corps

XIII.6.1 Centre d'un anneau ★

[Enoncé]

1. $Z(A) \subset A$ vérifie :
   - $0 \in Z(A)$ car $\forall a \in A,\ 0 \cdot a = 0 = a \cdot 0$
   - $1 \in Z(A)$ car $\forall a \in A,\ 1 \cdot a = a = a \cdot 1$;
   - $\forall (x,y) \in Z(A)^2,\ \forall a \in A,\ axy = xay = xya \implies xy \in A$;
   - $\forall (x,y) \in Z(A)^2,\ \forall a \in A,\ (x-y)a = xa-ya = ax-ay = a(x-y) \implies x-y \in Z(A)$.
   - $\forall (x,y) \in Z(A)^2,\ y \in A \implies xy = yx$.

   Ainsi $Z(A)$ est un sous-anneau commutatif de A.
2. Tout d'abord $(A,+,\times)$ est un anneau commutatif.
   Il reste à vérifier que $(A,+,\cdot)$ est un $Z(A)$-espace vectoriel. Si $(x,y) \in A^2$ et $(\lambda,\mu) \in Z(A)^2$ il est clair que :
   - $1 \cdot x = x$;
   - $(\lambda+\mu)\cdot x = \lambda x + \mu x$;
   - $\lambda \cdot (x+y) = \lambda \cdot x + \lambda \cdot y$;
   - $\lambda \cdot (\mu \cdot x) = (\lambda\mu) \cdot x$.

   Ainsi $(Z(A),+,\times,\cdot)$ est une $Z(A)$-algèbre unitaire, associative et commutative.

XIII.6.2 Calcul d'un inverse ★★★

[Enoncé]

1. Il existe $n \in \mathbb{N}^*$ tel que $(ab)^n = 0$.
   Alors $(ba)^{n+1} = (ba)(ba)\dots(ba) = b(ab)\dots(ab)a = b(ab)^n a = 0$. On s'inspire de la formule : $\forall x \in]-1,1[,\ (1-x)^{-1} = \sum_{k=0}^{+\infty} x^k$.
   Notons p l'indice de nilpotence de ab.
   $(1-ba)\sum_{k=0}^{p}(ba)^k = \sum_{k=0}^{p}(ba)^k - \sum_{k=0}^{p}(ba)^{k+1} = 1 + \sum_{k=1}^{p}(ba)^k - \sum_{k=1}^{p}(ba)^k = 1 + (ba)^{p+1} = 1$.
   De même, $\sum_{k=0}^{p}(ba)^k(1-ba) = 1$.
   Ainsi $1-ba$ est inversible et $(1-ba)^{-1} = \sum_{k=0}^{p}(ba)^k$.

On vérifie de même que $(1-ab)^{-1} = \sum_{k=0}^{p-1}(ab)^k$ de sorte que $(1-ba)^{-1} = 1+b\left(\sum_{k=0}^{p-1}(ab)^k\right)a = 1+b(1-ab)^{-1}a$.

2. Montrons que l'inverse de $(1-ba)$ est encore $1+b(1-ab)^{-1}a$.
$(1-ba)(1+b(1-ab)^{-1}a) = 1+b(1-ab)^{-1}a - ba - bab(1-ab)^{-1}a = 1-ba+b(1-ab)(1-ab)^{-1}a = 1-ba+ba = 1$. De même, $(1+b(1-ab)^{-1}a)(1-ba) = 1$.
Ainsi $(1-ba)$ est inversible et $(1-ba)^{-1} = 1+b(1-ab)^{-1}a$.

XIII.6.3 Anneau de Boole ★★

[Enoncé]
On rappelle que si A est une partie de E alors la fonction indicatrice de A est définie par $\mathbb{1}_A : \begin{cases} E & \longrightarrow & \{0,1\} \\ x & \longmapsto & \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{cases} \end{cases}$ et que $\forall (A,B) \in \mathcal{P}(E)^2,\ A = B \iff \mathbb{1}_A = \mathbb{1}_B$. On notera pour toute partie A de E, $\overline{A} = E\backslash A$ le complémentaire de A dans E ainsi que $1 = \mathbb{1}_E$.
On rappelle enfin les règles de calcul :

- $\mathbb{1}_{\overline{A}} = 1 - \mathbb{1}_A$;
- $\mathbb{1}_{A\cap B} = \mathbb{1}_A\mathbb{1}_B$;
- $\mathbb{1}_{A\cup B} = \mathbb{1}_A + \mathbb{1}_B - \mathbb{1}_A\mathbb{1}_B$.

1. Soit $(A,B,C) \in \mathcal{P}(E)^3$.
$\mathbb{1}_{A\Delta B} = \mathbb{1}_{A\backslash B} + \mathbb{1}_{B\backslash A}$ car $(A\backslash B)\cap(B\backslash A) = \emptyset$.
Donc $\mathbb{1}_{A\Delta B} = \mathbb{1}_{A\cap\overline{B}} + \mathbb{1}_{B\cap\overline{A}} = \mathbb{1}_A\mathbb{1}_{\overline{B}} + \mathbb{1}_B\mathbb{1}_{\overline{A}} = \mathbb{1}_A(1-\mathbb{1}_B) + \mathbb{1}_B(1-\mathbb{1}_A) = \mathbb{1}_A + \mathbb{1}_B - 2\mathbb{1}_A\mathbb{1}_B$.
On doit vérifier que $(\mathcal{P}(E),\Delta)$ est un groupe abélien :
   - Δ est une loi de composition interne : il est clair que $A\Delta B \in \mathcal{P}(E)$;
   - Δ est commutative : $A\Delta B = (A\backslash B)\cup(B\backslash A) = (B\backslash A)\cup(A\backslash B) = B\Delta A$;
   - Existence du neutre : $\emptyset\Delta A = A = A\Delta\emptyset$;
   - Tout élément est symétrisable (il n'y a même que des involution) : $A\Delta A = \emptyset$;
   - Δ est associative :

$$\begin{aligned}\mathbb{1}_{(A\Delta B)\Delta C} &= \mathbb{1}_{A\Delta B} + \mathbb{1}_C - 2\mathbb{1}_{A\Delta B}\mathbb{1}_C \\ &= \mathbb{1}_A + \mathbb{1}_B - 2\mathbb{1}_A\mathbb{1}_B + \mathbb{1}_C - 2(\mathbb{1}_A + \mathbb{1}_B - 2\mathbb{1}_A\mathbb{1}_B)\mathbb{1}_C \\ &= \mathbb{1}_A + \mathbb{1}_B + \mathbb{1}_C - 2(\mathbb{1}_A\mathbb{1}_B + \mathbb{1}_A\mathbb{1}_C + \mathbb{1}_B\mathbb{1}_C) + 4\mathbb{1}_A\mathbb{1}_B\mathbb{1}_C\end{aligned}$$

Et

$$\begin{aligned}\mathbb{1}_{A\Delta(B\Delta C)} &= \mathbb{1}_A + \mathbb{1}_{B\Delta C} - 2\mathbb{1}_A\mathbb{1}_{B\Delta C}\\ &= \mathbb{1}_A + \mathbb{1}_B + \mathbb{1}_C - 2\mathbb{1}_B\mathbb{1}_C - 2\mathbb{1}_A(\mathbb{1}_B + \mathbb{1}_C - 2\mathbb{1}_B\mathbb{1}_C)\\ &= \mathbb{1}_A + \mathbb{1}_B + \mathbb{1}_C - 2(\mathbb{1}_A\mathbb{1}_B + \mathbb{1}_A\mathbb{1}_C + \mathbb{1}_B\mathbb{1}_C) + 4\mathbb{1}_A\mathbb{1}_B\mathbb{1}_C\end{aligned}$$

Ensuite il faut que la loi $\cap$ soit distributive sur la loi Δ :
$\mathbb{1}_{A\cap(B\Delta C)} = \mathbb{1}_A\mathbb{1}_{B\Delta C} = \mathbb{1}_A(\mathbb{1}_B + \mathbb{1}_C - 2\mathbb{1}_C\mathbb{1}_B) = \mathbb{1}_A\mathbb{1}_B + \mathbb{1}_A\mathbb{1}_C - 2\mathbb{1}_A\mathbb{1}_B\mathbb{1}_C = \mathbb{1}_{A\cap B} + \mathbb{1}_{A\cap C} - 2\mathbb{1}_{A\cap B}\mathbb{1}_{A\cap C} = \mathbb{1}_{(A\cap B)\Delta(A\cap C)}$.
L'avant dernière égalité est obtenue en utilisant $\mathbb{1}_A^2 = \mathbb{1}_{A\cap A} = \mathbb{1}_A$ et en écrivant $\mathbb{1}_A\mathbb{1}_B\mathbb{1}_C = \mathbb{1}_A^2\mathbb{1}_B\mathbb{1}_C = (\mathbb{1}_A\mathbb{1}_B)(\mathbb{1}_A\mathbb{1}_C)$.
Puis la loi $\cap$ doit être associative et commutative :

— $A \cap B = B \cap A$;
— $(A \cap B) \cap C = A \cap (B \cap C)$.

Enfin la loi $\cap$ doit posséder un neutre (différent de celui de la loi Δ) :
$A \cap E = A = E \cap A$ et $E \neq \emptyset$.

Finalement $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif.
Remarque : En prenant un peu de recul on peut faire une analogie entre la différence symétrique et les portes logiques dans l'algèbre de Boole. L'opération de différence symétrique représente la porte "XOR" ou le "OU exclusif" (A ou B, mais pas les deux). Plus classiquement l'opération d'intersection traduit le "ET" ou la porte "AND". C'est l'origine de l'appellation anneau de Boole pour cet anneau et cela permet de mieux saisir la structure de ces opérations ainsi que leurs interactions.

2. Soit $A \subset E$ inversible pour la loi $\cap$. On note B l'inverse de A.
On sait que $A \cap B = E$. Si $A \subsetneq E$ alors $A \cap B \subset A \implies A \cap B \neq E$. Donc $A = E$.
Le neutre est toujours inversible donc E est le seul élément de $(\mathcal{P}(E), \Delta, \cap)$ inversible pour la loi $\cap$.
3. On cherche à montrer ou réfuter la proposition "$\forall (A, B) \in \mathcal{P}(E)^2,\ A \cap B = \emptyset \implies A = \emptyset \vee B = \emptyset$".
S'il existe une partie A de E non vide et non égale à E en entier, autrement dit si E n'est pas un singleton, alors $A \cap \overline{A} = \emptyset$ avec $A \neq \emptyset$ et $\overline{A} \neq \emptyset$.
Dans le cas contraire on note $E = \{x\}$. On a alors $\mathcal{P}(E) = \{\emptyset, \{x\}\}$. Dans ces conditions il est clair que $\forall (A, B) \in \mathcal{P}(E)^2,\ A \cap B = \emptyset \implies A = \emptyset \vee B = \emptyset$.
Par conséquent $(\mathcal{P}(E), \Delta, \cap)$ est un anneau intègre si et seulement si E ne possède qu'un seul élément.

L'anneau de Boole est principal ★★★

Soit $F \subset E$. $\emptyset \in \mathcal{P}(F)$.
Si $(A, B) \in \mathcal{P}(F)^2$ alors $A\Delta B \subset A \cup B \subset F$, c'est à dire $A\Delta B \in \mathcal{P}(F)$. Trivialement le symétrique de A reste dans $\mathcal{P}(F)$ puisque que c'est lui-même. Donc $\mathcal{P}(F)$ est un sous groupe

de $(\mathcal{P}(E), \Delta)$. De plus si $C \subset E$ alors $A \cap C \subset A \subset F$ donc $A \cap C \in \mathcal{P}(F)$: $\mathcal{P}(F)$ est absorbant.
On en déduit que $\mathcal{P}(F)$ est un idéal de $\mathcal{P}(E)$.

Donnons nous maintenant un idéal I de $\mathcal{P}(E)$.
Comme E est fini, l'ensemble $M = \{\text{Card}(A),\ A \in I\}$ est majoré par $\text{Card}(E)$. C'est une partie majorée de $\mathbb{N}$, elle admet donc un maximum. On note F tel que $\text{Card}(F) = \max(M)$.
Montrons que $I = \mathcal{P}(F)$.
Pour cela on va montrer que I est stable par réunion. Fixons $(A, B) \in I^2$. D'un point de vue logique, il s'agit de construire la porte "OR" à partir des portes "AND" et "XOR".
Intuitivement $A\Delta(\overline{A} \cap B)$ à l'air de fonctionner.
On vérifie :
$\mathbb{1}_{A\Delta(\overline{A}\cap B)} = \mathbb{1}_A + \mathbb{1}_{\overline{A}\cap B} - \mathbb{1}_A\mathbb{1}_{\overline{A}\cap B} = \mathbb{1}_A + \mathbb{1}_{\overline{A}}\mathbb{1}_B - \mathbb{1}_A\mathbb{1}_{\overline{A}}\mathbb{1}_B = \mathbb{1}_A + (1-\mathbb{1}_A)\mathbb{1}_B - \mathbb{1}_{A\cap\overline{A}}\mathbb{1}_B = \mathbb{1}_1 + \mathbb{1}_B - \mathbb{1}_A\mathbb{1}_B = \mathbb{1}_{A\cup B}$.
$\overline{A} \cap B \in I$ par absorbance et $A \in I$ donc $A \cup B = A\Delta(\overline{A} \cap B) \in I$.
Ainsi si $F' \in I$ alors $F \cup F' \in I$. Si F' n'est pas inclus dans F alors $F' \cup F$ a un cardinal strictement plus grand que celui de F ce qui contredit la maximalité de $\text{Card}(F)$ dans M.
Donc $F' \in \mathcal{P}(F)$.
Réciproquement si $F' \subset F$ alors $F' = F' \cap F \in I$ par absorbance.
Finalement $I = \mathcal{P}(F)$.

Remarque : on a montré que l'anneau $(\mathcal{P}(E), \Delta, \cap)$ est principal (cf. VI.8).

XIII.6.4 Condition suffisante pour qu'un anneau soit commutatif ★★★

[Enoncé]

1. Soit $(x, y) \in A^2$.
   $x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$ donc $xy = -yx = (-yx)^2 = (yx)^2 = yx$.
2. a. Soit $x \in A$ nilpotent. Par récurrence double immédiate $\forall n \in \mathbb{N}^*,\ x^n \in \{x, x^2\}$. Donc $x = 0$ ou $x^2 = 0$. Dans tous les cas $x = x^3 = 0$.
   Le seul élément nilpotent de A est 0.
   b. $b^2 = ea(1-e) \cdot ea(1-e) = (ea - eae)ea(1-e) = (eae - eae)a(1-e) = 0$.
   On en déduit que b est nul c'est à dire $ea = eae$.
   En considérant de même $c = (1-e)ae$ on obtient $ae = eae$. Il en résulte que a et e commute. Ainsi $e \in Z(A)$.
   Soit $x \in A$. $(x^2)^2 = x^4 = x^2$ donc d'après ce qui précède, $x^2 \in Z(A)$.
   c. On montre que $Z(A)$ est un sous-anneau (cf. VI.1). Fixons $x \in A$.
   Alors $2x = (x+1)^2 - x^2 - 1 \in Z(A)$ et $3x = (x+1)^3 - x^3 - 3x^2 - 1 = x + 1 - x - 3x^2 - 1 = -3x^2 \in Z(A)$.

Ainsi $x = 3x - 2x \in Z(A)$. On en déduit que $Z(A) = A$ c'est à dire que A est commutatif.

XIII.6.5 Anneaux commutatifs ou anti-commutatifs ★★★★

[Enoncé]

On considère $Z = \{x \in A,\ \forall a \in ax = xa\}$ et $Y = \{x \in A,\ \forall a \in A,\ ax = -xa\}$. On montre aisément que Z et Y sont des sous-groupes de $(A, +)$.
Montrons que $A = Z \cup Y$. Il est évident que $Z \cup Y \subset A$. Supposons par l'absurde qu'il existe $x \in A \backslash (Z \cup Y)$.
Comme $x \notin Z$, il existe $a \in A$ tel que $xa \neq ax$. Donc $xa = -ax$.
Comme $x \notin Y$, il existe $b \in A$ tel que $xb \neq -bx$. Donc $xb = bx$.
Alors $(b + a)x = x(b - a)$. Or par hypothèse, $(b + a)x \in \{x(b + a), -x(b + a)\}$.
Si $(b + a)x = x(b + a)$ alors $xb - xa = xb + xa$ d'où $2xa = 0$ c'est à dire $xa = -xa = ax$ ce qui est contraire à la définition de a.
De même, si $(a + b)x = -x(a + b)$ alors $bx = -xb$ ce qui est contraire à la définition de b.
On a montré que $A = Z \cup Y$. Or il est classique de montrer que l'union de deux sous-groupe est un sous-groupe si et seulement si l'un des deux contient l'autre (cf V.6). Comme $Z \cap Y = \emptyset$, cela impose $Y = \emptyset$ ou $Z = \emptyset$ autrement dit A est commutatif ou anti-commutatif.

Supposons maintenant que $(A, +, \times)$ est un anneau. Supposons que A est anti-commutatif.
Alors $\forall x \in A,\ x = 1_A x = -x1_A = -x$. Ainsi $\forall (x, y) \in A^2,\ xy = -yx = yx$.
Dans tous les cas A est commutatif.

XIII.6.6 Anneau régulier ★★★★

[Enoncé]

1. $(\mathbb{Z}, +, \times)$ n'est pas régulier, par exemple il n'existe pas d'entier u tel que $2 \times u \times 2 = 2$.
2. Soit $(K, +, \times)$ un corps.
   - $0_K \times 0_K \times 0_K = 0_K$;
   - Si $a \in K \backslash \{0_K\}$ alors a est inversible et $a^{-1} \in K$ et $aa^{-1}a = a$.

   Un corps est régulier.
3. a. Soit $(a, b) \in A \times B$. On sait qu'il existe $(u, v) \in A \times B$ tel que $aua = a$ et $bvb = b$. Donc $(a, b)(u, v)(a, b) = (aua, bvb) = (a, b)$ d'où $A \times B$ est régulier.
   b. Excluons les cas triviaux $n = 0$ et $n = 1$ où $\mathbb{Z}/0\mathbb{Z}$ est isomorphe à $\mathbb{Z}$ et est donc régulier et $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$ est clairement régulier. Fixons $n \geq 2$.
   Si p est un nombre premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps et est donc régulier d'après la question 2. Si n est *quadratfrei*, c'est à dire qu'il s'écrit comme un produit de nombres premiers distinct $n = p_1 \dots p_k$ alors d'après le théorème des restes chinois $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\mathbb{Z}/p_1\mathbb{Z} \times \dots \times \mathbb{Z}/p_k\mathbb{Z}$. Ce dernier anneau est régulier par récurrence sur la question 3.*a* donc $\mathbb{Z}/n\mathbb{Z}$ est régulier.

Supposons maintenant qu'il existe un nombre premier p tel que $p^2|n$. Supposons par l'absurde que $\mathbb{Z}/n\mathbb{Z}$ est régulier.
Alors $\exists u \in \mathbb{Z},\ \overline{p} \times \overline{u} \times \overline{p} = \overline{up^2} = \overline{p}$. C'est à dire $\exists (u,v) \in \mathbb{Z}^2,\ p = up^2 + vn$.
Or $p^2|up^2 + vn$ donc $p^2|p$ ce qui est absurde. Finalement, $\mathbb{Z}/n\mathbb{Z}$ est régulier si et seulement si $n = 0,\ n = 1$ ou $n \geq 2$ et est quadratfrei.

4. a. Soit $u \in \mathcal{L}(E)$. On pose S un supplémentaire de $\mathrm{Ker}(u)$.
On sait d'après le théorème du rang que $\tilde{u} = u_{|S}^{|\mathrm{Im}(u)}$ est un isomorphisme.
On définit alors v sur $E = S \oplus \mathrm{Ker}(u)$ par $v(x) = \begin{cases} 0 & \text{si } x \in \mathrm{Ker}(u) \\ \tilde{u}^{-1}(x) & \text{si } x \in S \end{cases}$.
v est bien un endomorphisme de E et,
— $\forall x \in \mathrm{Ker}(u),\ u \circ v \circ u(x) = 0 = u(x)$;
— $\forall x \in S,\ u \circ v \circ u(x) = u \circ \tilde{u}^{-1}(\tilde{u}(x)) = u(x)$.
Donc $u \circ v \circ u = u$.

b. Notons φ l'endomorphisme associé à A dans la base canonique notée $(e_1, \dots, e_n)$.
On a $\mathrm{Ker}(\varphi) = \mathrm{Ker}(A) = \mathrm{Vect}(e_1)$ et $\mathrm{Im}(\varphi) = \mathrm{Im}(A) = \mathrm{Vect}(e_1, \dots, e_{n-1})$. Donc en posant $S = \mathrm{Vect}(e_2, \dots, e_n)$, on a $\mathrm{Ker}(A) \oplus S = \mathcal{M}_{n,1}(\mathbb{K})$.
On pose $\tilde{\varphi} = \varphi_{|S}^{|\mathrm{Im}(\varphi)}$. On sait que $\tilde{\varphi}$ est un isomorphisme, déterminons son inverse.
$\forall i \in [\![2; n]\!],\ \tilde{\varphi}(e_i) = e_{i-1}$. Ainsi $\tilde{\varphi}^{-1}$ est définie par $\forall i \in [\![1; n-1]\!],\ \tilde{\varphi}^{-1}(e_i) = e_{i+1}$.
On définit enfin u sur $E = S \oplus \mathrm{Ker}(\varphi)$ par $u(e_n) = 0$ et $\forall i \in [\![1; n-1]\!],\ u(e_i) = e_{i+1}$ et on a $\varphi \circ u \circ \varphi = \varphi$.
Donc en notant $U = \mathrm{Mat}_{(e_1,\dots,e_n)}(u) = \left(\begin{array}{cccc|c} 0 & \cdots & \cdots & 0 & 0 \\ \hline 1 & 0 & \cdots & 0 & 0 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{array}\right)$ on a $AUA = A$.

5. Soit A un anneau régulier. Notons Z le centre de A et fixons $a \in Z$. Comme $a \in A$, il existe $u \in A$ tel que $aua = a$. On cherche $v \in Z$ tel que $ava = a$. On va montrer que $v = uau$ convient.
Tout d'abord, $ava = a(uau)a = (aua)ua = aua = a$. Fixons ensuite $b \in A$. Comme $a \in Z$,
$(1 - au)bau = (a - aua)bu = 0$ et $aub(1 - au) = ub(a - aua) = 0$.
Donc $bau - aubau = 0 = aub - aubau$ c'est à dire $bau = aub$.
Ainsi $vb = uaub = ubau = aubu = bau^2 = bv$.

XIII.6.7 Anneau intègre fini ★

[Enoncé]
Il s'agit de montrer que tout élément non nul de A est inversible. Fixons $a \in A \backslash \{0_A\}$.
On sait que $\forall n \in \mathbb{N}^*,\ a^n \in A$. Comme A est fini, on en déduit qu'il existe deux entiers naturels non nuls $p > q$ tels que $a^q = a^p$.

Mais alors $a^q - a^p = 0$ c'est à dire $a^p(a^{q-p} - 1) = 0$ c'est à dire $a^p = 0$ ou $a^{q-p} = 1$ par intégrité. Encore par intégrité, $a^p = 0 \implies a = 0$.
Donc $a^{p-q} = 1$. On en déduit que a est inversible d'inverse a^{p-q-1} qui est bien défini puisque $p - q - 1 \geq 0$.

XIII.6.8 Anneau principal (1) ★★★

[Enoncé]

1. L'idéal nul $\{0\} = 0\mathbb{Q}$ est évidemment principal. Soit I un idéal non nul de $\mathbb{Q}$.
   Il existe $a \in I$ non nul. Alors $a \times \dfrac{1}{a} = 1 \in I$ par absorbance. Mais alors quel que soit $b \in \mathbb{Q}$, $b = 1 \times b \in I$ par absorbance. Donc $I = \mathbb{Q} = 1\mathbb{Q}$.
   Ainsi $(\mathbb{Q}, +, \times)$ est principal.
   Remarque : On peut en fait montrer de manière plus général que les seuls idéaux d'un corps sont l'idéal nul et le corps tout entier (cf. XIII.6.14) et donc en particulier qu'un corps est toujours un anneau principal
2. Un idéal de $(\mathbb{Z}, +, \times)$ est avant tout un sous-groupe de $(\mathbb{Z}, +)$. Or on montre classiquement que les sous-groupes de $\mathbb{Z}$ sont les $a\mathbb{Z}$ pour $a \in \mathbb{Z}$ (cf. V.11). On en déduit que $(\mathbb{Z}, +, \times)$ est principal.
3. Soit I un idéal non nul de $\mathbb{D}$. On se donne $x \in I \backslash \{0\}$. Quitte à considérer $-x$ on peut supposer $x > 0$. On écrit $x = \dfrac{a}{10^n}$ avec $a \in \mathbb{N}^*$ et $n \in \mathbb{N}$.
   Par absorbance, $a = x \times 10^n \in I$ donc $a \in I \cap \mathbb{N}^*$. Posons $\alpha = \min(I \cap \mathbb{N}^*)$. Le minimum existe car il s'agit d'une partie non vide de $\mathbb{N}$. $\alpha \in I \implies \alpha\mathbb{D} \subset I$.
   Réciproquement fixons $y = \dfrac{b}{10^m} \in I$. $b = y \times 10^m \in I \cap \mathbb{Z}$. Notons $b = \alpha q + r$ la division euclidienne de b par α. Comme $b \in I$ et $\alpha \in I$, $r = b - \alpha q \in I$.
   Or si $r > 0$ alors $r \in I \cap \mathbb{N}^*$ et $r < \alpha$ ce qui absurde. Donc $r = 0$ et $b \in \alpha\mathbb{Z}$.
   On en déduit que $y = \dfrac{b}{10^m} \in \alpha\mathbb{D}$. Ainsi $I = \alpha\mathbb{D}$ et $\mathbb{D}$ est principal.

   Plus précisément on sait que le numérateur dans l'écriture d'un nombre décimal $x = \dfrac{a}{10^n}$ peut toujours être pris entre 0 et 9. Notons $C = \{a \in [\![0; 9]\!],\ a \in I\}$
   - Si $a \in C \cap \{1, 2, 4, 5, 8\}$ alors $\dfrac{1}{a} \in \mathbb{D}$ d'où $1 \in I$ puis $I = \mathbb{D}$ par absorbance.
   - Si $6 \in C$ alors $3 = 6 \times \dfrac{1}{2} \in I$ donc $6\mathbb{D} = 3\mathbb{D}$.

   Finalement les seuls idéaux de $\mathbb{D}$ sont $\{0\}$, $3\mathbb{D}$, $7\mathbb{D}$, $9\mathbb{D}$ et $\mathbb{D}$.
4. Comme $\forall (d, k) \in \mathbb{Z}^2$, $d\overline{k} = \overline{d} \times \overline{k}$, les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$. Or $\mathbb{Z}/n\mathbb{Z}$ est cyclique en tant que groupe additif (il est engendré par $\overline{1}$). On montre alors (cf. V.32) que ses sous-groupes sont cycliques. Autrement dit ses idéaux sont principaux et $\mathbb{Z}/n\mathbb{Z}$ est un anneau principal.

XIII.6.9 Anneau principal (2) ★★★

[Enoncé]

1. D'après le cours les sous-groupes de $(\mathbb{Z},+)$ sont les $a\mathbb{Z}$ pour $a\in\mathbb{Z}$. Un idéal de $\mathbb{Z}$ étant avant tout un sous-groupe additif de $\mathbb{Z}$, $(\mathbb{Z},+,\times)$ est principal.
2. Considérons $I=2\mathbb{Z}[X]+X\mathbb{Z}[X]$. Supposons que $I=P\mathbb{Z}[X]$ pour un certain $P\in\mathbb{Z}[X]$. Alors $P|2\in I$ d'où $P\in\{-2,-1,1,2\}$. Or 2 ne divise pas X dans $\mathbb{Z}[X]$ donc $P=\pm1$.
   On peut alors trouver $U,V\in\mathbb{Z}[X]$ vérifiant $1=2U+XV$. En évaluant en 0 on obtient $1=2U(0)$ ce qui est absurde car $U(0)\in\mathbb{Z}$.
   Ainsi $\mathbb{Z}[X]$ n'est pas principal.
3. D'après les questions précédentes la condition "A est principal" n'est pas suffisante pour assurer la principalité de $A[X]$. On sait par contre d'après le cours que $\mathbb{K}[X]$ est principal pour $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$. On conjecture alors que A doit être un corps. On va s'inspirer de la démonstration faîte pour $\mathbb{C}[X]$ et $\mathbb{R}[X]$.
   Supposons que A est un corps et donnons nous I un idéal de $A[X]$. Si I est nul alors il est principal, on suppose donc dans la suite que ce n'est pas le cas. L'ensemble des degrés des polynômes non nuls de I est une partie non vide de $\mathbb{N}$, elle admet donc un minimum. On pose Π qui réalise ce minimum. Montrons que $I=\Pi A[X]$.
   On a déjà $\Pi A[X]\subset I$ par absorbance. Pour montrer l'inclusion réciproque dans le cas $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$ on réalise des divisions euclidiennes par Π. Montrons un résultat similaire dans $A[X]$:

$$\forall P\in A[X],\ \exists(Q,R)\in A[X],\ (P=Q\Pi+R\wedge\deg(R)<\deg(\Pi))$$

   Fixons $P=\sum_{k=0}^{d_0}a_kX^k\in I\backslash\{0\}$ avec $d_0:=\deg(P)$.
   $\Pi=\sum_{k=0}^{p}b_kX^k$ est non nul donc $p:=\deg(\Pi)\in\mathbb{N}$. Si $p>d_0$ alors $P=0\times\Pi+P$ fait l'affaire. Sinon, on considère $P_1(X)=P(X)-a_{d_0}b_p^{-1}X^{d_0-p}\Pi(X)\in A[X]$ car A est un corps. Par construction $d_1:=\deg(P_1)<d_0$. Si $d_1<p$ alors $P=a_{d_0}b_p^{-1}X^{d_0-p}\Pi+P_1$ fait l'affaire. Sinon on réitère le processus en remplaçant P par P_1 etc...
   Finalement on peut trouver des polynômes Q et R comme voulus.
   Maintenant, R ne peut qu'être nul puisque sinon il contredirait la minimalité du degré de Π dans $I\backslash\{0\}$. Par conséquent $R=0$ et $P=Q\Pi\in\Pi A[X]$. Ainsi $I=\Pi A[X]$ est principal et par suite, $A[X]$ est principal.

   Pour montrer le sens réciproque on va raisonner par contraposition. Supposons que A n'est pas un corps. On se donne un élément a non nul et non inversible de A. On considère comme dans la question précédente $I=aA[X]+XA[X]$.
   Si $A[X]$ est principal alors il existe $P\in A[X]$ tel que $I=PA[X]$. Dans ce cas $P|a\in I$

donc P est constant. De plus $P|X \in I$ donc $\exists Q \in A[X],\ PQ = X$. Q est forcément un monôme de degré 1 et donc en identifiant les coefficients on a $P|1$ d'où $1 \in I$.
On en déduit qu'on peut trouver deux polynômes $U, V \in A[X]$ vérifiant $1 = aU + VX$. En évaluant en 0 on obtient que a est inversible d'inverse $U(0) \in A$ ce qui est absurde.

Finalement, $A[X]$ est principal si et seulement si A est un corps.

XIII.6.10 Anneau euclidien ★★

[Enoncé]

1. $\mathbb{Z}$ est un anneau euclidien en considérant pour $(a, b) \in \mathbb{Z} \times \mathbb{Z}\backslash\{0\}$ la division euclidienne de a par $|b|$ et φ l'application $x \in \mathbb{Z} \mapsto |x|$.
   $\mathbb{K}[X]$ est euclidien en considérant la division euclidienne de deux polynômes et φ l'application $P \in \mathbb{K}[X] \mapsto \deg(P)$.
2. Soit A un anneau euclidien. Soit I un idéal de A. Si $I = \{0_A\}$ alors $I = 0_A A$. Si $I \neq \{0\}$ alors on se donne un élément $x \in I$ non nul. Considérons $E = \{\varphi(a), a \in I\backslash\{0_A\}\}$. E admet un minimum en tant que partie non vide de $\mathbb{N}$. On note $b \in A$ qui réalise ce minimum. $bA \subset I$ par absorbance. Fixons $a \in A$.
   On sait qu'il existe un couple $(q, r) \in A^2$ tel que $a = bq + r$ et $(r = 0_A$ ou $\varphi(r) < \varphi(b))$.
   Supposons que $r \neq 0_A$. Alors comme $b \in I$, $bq \in I$ puis comme I est un sous-groupe additif de A, $r = a - bq \in I$. Cependant $\varphi(r) < \varphi(b)$ ce qui contredit la minimalité de $\varphi(b)$. On en déduit que $r = 0_A$ et que $a = bq \in bA$.
   Ainsi $I = bA$ et A est principal.

XIII.6.11 Entiers de Gauss ★★★★★

[Enoncé]

1. Tout d'abord $\mathbb{Z}[i] \subset \mathbb{C}$ qui est un anneau commutatif intègre.
   Ensuite $0 = 0 + 0i \in \mathbb{Z}[i]$ et $1 = 1 + 0i \in \mathbb{Z}[i]$. Fixons $(x, y) \in \mathbb{Z}[i]$. Il existe $a, b, c, d \in \mathbb{Z}$ tel que $x = a + ib$ et $y = c + id$.
   D'une part $x - y = a - c + i(b - d) \in \mathbb{Z}[i]$ car $(a - c, b - d) \in \mathbb{Z}^2$, d'autre part $xy = ac - bd + i(ad + bc) \in \mathbb{Z}[i]$ car $(ac - bd, ad + bc) \in \mathbb{Z}^2$.
   Ainsi $\mathbb{Z}[i]$ est un anneau commutatif intègre en tant que sous anneau d'un anneau commutatif intègre.
2. Soit $x = a + ib \in \mathbb{Z}[i]$ inversible. Alors x est inversible dans $\mathbb{C}$ d'où $x^{-1} = \dfrac{1}{a + ib} = \dfrac{a - ib}{a^2 + b^2}$ et de plus $x^{-1} \in \mathbb{Z}[i]$ donc $\dfrac{a}{a^2 + b^2} \in \mathbb{Z}$ et $\dfrac{b}{a^2 + b^2} \in \mathbb{Z}$.
   Or si $b \neq 0$ alors $a^2 + b^2 > a^2 \geq |a|$ d'où $\dfrac{a}{a^2 + b^2} \in \mathbb{Z} \implies a = 0$. On a alors $\dfrac{1}{b} \in \mathbb{Z}$ d'où $b = \pm 1$.

De même si $a \neq 0$ alors $b = 0$ et $a = \pm 1$.
De plus $1, -1, i, -i$ sont inversible dans $\mathbb{Z}[i]$ (d'inverse respectif $1, -1, -i, i$) donc $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

3. Soit $(x, y) \in \mathbb{Z}[i] \times \mathbb{Z}[i] \backslash \{0\}$. Notons $\dfrac{x}{y} = u + iv$ avec $u, v \in \mathbb{R}$. On pose $q = a + ib$ où a est l'entier le plus proche de u et b l'entier le plus proche de v. q est donc dans $\mathbb{Z}[i]$ et de plus $|u - a| \leq \dfrac{1}{2}$ et $|v - b| \leq \dfrac{1}{2}$.
Par conséquent $N\left(\dfrac{x}{y} - q\right) = N(u-a+i(v-b)) = (u-a)^2+(v-b)^2 \leq \left(\dfrac{1}{2}\right)^2+\left(\dfrac{1}{2}\right)^2 = \dfrac{1}{2} < 1$ ou encore $N(x - qy) < N(y)$.
Ainsi on a $x = qy + r$ avec $q \in \mathbb{Z}[i], r = x - qy \in \mathbb{Z}[i]$ et $N(r) < N(y)$ où $N : x = a + ib \in \mathbb{Z}[i] \mapsto |x|^2 = a^2 + b^2 \in \mathbb{N}$ ce qui montre que $\mathbb{Z}[i]$ est euclidien.
On montre alors (cf. VI.10) qu'il est principal.

4. a. Soit $a \in \mathbb{Z}[i]$ tel que $N(a)$ est un nombre premier. Fixons $(b, c) \in \mathbb{Z}[i]^2$ tel que $a = bc$.
Alors $N(a) = N(b)N(c)$. Or $N(a)$ étant premier, on sait que $(N(b), N(c)) \in \{(1, N(a)), (N(a), 1)\}$. On a montré dans la question 1 que $x \in \mathbb{Z}[i]^\times \iff N(x) = 1$. Ainsi on a bien $b \in \mathbb{Z}[i]^\times$ ou $c \in \mathbb{Z}[i]^\times$ d'où a est irréductible dans $\mathbb{Z}[i]$.

   b. (i) $\Longrightarrow$ (ii) :
Raisonnons pas l'absurde, si $p \not\equiv 3[4]$ alors $\exists x \in \mathbb{Z},\ x^2 \equiv -1[p]$. Donc p divise $x^2 + 1 = (x - i)(x + i)$ dans $\mathbb{Z}$ et donc dans $\mathbb{Z}[i]$. p est irréductible dans $\mathbb{Z}[i]$ donc p divise $x - i$ ou p divise $x + i$ dans $\mathbb{Z}[i]$. Or ceci est impossible puisque $\dfrac{x}{p} - \dfrac{i}{p}$ et $\dfrac{x}{p} + \dfrac{i}{p}$ ne sont pas des éléments de $\mathbb{Z}[i]$.
(ii) $\Longrightarrow$ (iii) :
Encore une fois par l'absurde, supposons qu'il existe $x = a + ib \in \mathbb{Z}[i]$ tel que $p = N(x) = a^2 + b^2$. On remarque qu'un carré est toujours congrus à 0 ou 1 modulo 4 (il suffit de faire tous les cas). Donc p ne peut être congrus qu'à 0, 1 ou 2 modulo 4 ce qui est absurde.
(iii) $\Longrightarrow$ (i) :
Toujours par l'absurde, soit $(a, b) \in \mathbb{Z}[i]^2$ tel que $p = ab$. On a $p^2 = N(p) = N(ab) = N(a)N(b)$. Si a et b ne sont pas inversibles alors $N(a)$ et $N(b)$ sont tous deux différents de 1. On en déduit comme p est premier que $N(a) = N(b) = p$. Mais alors $p^2 = N(a)^2$ d'où $p = N(a)$ ce qui est absurde.

   c. D'après les questions précédentes on sait déjà que les entiers premiers congrus à 3 modulo 4 et les éléments a de $\mathbb{Z}[i]$ tels que $N(a)$ soit premier sont irréductibles dans $\mathbb{Z}[i]$. Montrons que ce sont les seuls.
Soit x irréductible dans $\mathbb{Z}[i]$. On remarque que x divise $N(x) > 1$ dans $\mathbb{Z}[i]$. $N(x)$ s'écrit comme un produit de puissance de nombre premier. Puisque x est irréductible, il divise un de ces nombres premiers p (dans $\mathbb{Z}[i]$). Autrement dit $\exists y \in \mathbb{Z}[i],\ p = xy$. Et donc $p^2 = N(x)N(y)$. Puisque $N(x) \neq 1$ on sait que

$N(x) = p$ ou $N(x) = p^2$. Si $N(x) = p^2$ alors $N(y) = 1$ c'est à dire y est inversible dans $\mathbb{Z}[i]$ c'est à dire p est irréductible dans $\mathbb{Z}[i]$ (il est associé à x) et donc p est congrus à 3 modulo 4 d'après la question précédente. Et si $N(x) = p$ alors $N(y) = p$ et $p^2 = N(x)^2$ d'où $N(x) = p$ est premier.

5. On montre classiquement que la relation $\sim$ définie par : $\forall (x, y) \in \mathbb{Z}[i]^2,\ x \sim y \iff \exists e \in \mathbb{Z}[i]^\times,\ x = ey$ est une relation d'équivalence sur $\mathbb{Z}[i]$. D'après la question 1, si $x \in \mathbb{Z}[i]$ alors sa classe d'équivalence est $C_x = \{x, -x, ix, -ix\}$. On remarque que si $x \in \mathbb{Z}[i]$ alors $\forall y \in C_x,\ N(y) = N(x)$. On va donc partitionner la somme suivant la décomposition $\{x \in \mathbb{Z}[i],\ N(x) = n\} = \bigsqcup_{i=1}^{p} C_{a_i}$ où les C_{a_i} sont les classes d'équivalence de la relation $\sim$:
$S_{n,k} = \dfrac{1}{4} \displaystyle\sum_{\substack{x \in \mathbb{Z}[i] \\ N(x)=n}} x^k = \frac{1}{4} \sum_{i=1}^{p} a_i^k \left(1^k + (-1)^k + i^k + (-i)^k\right)$.
Or la valeur de la somme $s_k = 1^k + (-1)^k + i^k + (-i)^k$ est déterminée par la classe de k dans $\mathbb{Z}/4\mathbb{Z}$:
   — Si $k \equiv 0[4]$ alors $s_k = 4$;
   — Si $k \equiv 1[4]$ alors $s_k = 0$;
   — Si $k \equiv 2[4]$ alors $s_k = 0$;
   — Si $k \equiv 3[4]$ alors $s_k = 0$.

   Finalement, $S_{n,k} = \begin{cases} \displaystyle\sum_{i=1}^{p} a_i^k & \text{si } 4|k \\ 0 & \text{sinon} \end{cases}$.
   Dans tous les cas, $S_{n,k} \in \mathbb{Z}[i]$.
   De plus, $\overline{S}_{n,k} = \dfrac{1}{4} \displaystyle\sum_{\substack{x \in \mathbb{Z}[i] \\ N(x)=n}} \overline{x}^k = \frac{1}{4} \sum_{\substack{\overline{x} \in \mathbb{Z}[i] \\ N(\overline{x})=n}} x^k = \frac{1}{4} \sum_{\substack{x \in \mathbb{Z}[i] \\ N(x)=n}} x^k = S_{n,k}$.
   On en déduit que la partie imaginaire de $S_{n,k}$ est nulle et donc que $S_{n,k} \in \mathbb{Z}$.

XIII.6.12 Anneau Noethérien ★★★★

[Enoncé]

1. Soit $(A, +, \times)$ un anneau commutatif.
   (i) $\implies$ (ii) :
   On suppose A noethérien et on se donne $(I_n)_{n\in\mathbb{N}}$ une suite d'idéaux de A croissante pour l'inclusion, c'est à dire que $\forall n \in \mathbb{N},\ I_n \subset I_{n+1}$.
   Notons $N = \displaystyle\bigcup_{n\in\mathbb{N}} I_n$. Montrons que N est un idéal de A :
   — $0_A \in I_0 \implies 0_A \in N$;

— Si $(x,y) \in N^2$ alors il existe $n,m \in \mathbb{N}$ tels que $x \in I_n$ et $y \in I_m$. Alors $(x,y) \in I^2_{\max(m,n)}$ d'où $x+y \in I_{\max(m,n)}$ puis $x+y \in N$;
— Si $a \in A$ et $x \in N$ alors il existe $n \in \mathbb{N}$ tel que $x \in I_n$. Alors $ax \in I_n$ par absorbance puis $ax \in N$.

On en déduit, comme A est noethérien, que N est engendré par une famille $(a_i)_{i\in[\![1;p]\!]}$ de A finie.
Chacun des éléments de la famille appartient à N, il existe donc pour tout $i \in [\![1;p]\!]$ un entier naturel n_i pour lequel $a_i \in I_{n_i}$. Ainsi $(a_i)_{i\in[\![1;p]\!]}$ est une famille de I_m pour $m = \max(n_1,\dots,n_p)$. On en déduit que la partie engendré par cette famille, qui est N, est contenue dans I_m. Ainsi $N = I_m$ et donc $(I_n)_{n\in\mathbb{N}}$ stationne à I_m.

(ii) $\implies$ (iii) :
On raisonne par contraposé. Supposons qu'il existe un ensemble non vide E d'idéaux de A qui n'admet pas d'élément maximal. Soit $I_0 \in E$. On suppose qu'il existe pour un certain $p \in \mathbb{N}$ une famille $(I_n)_{n\in[\![1;p]\!]}$ de E vérifiant $\forall n \in [\![0;p-1]\!],\ I_n \subsetneq I_{n+1}$. Alors comme I_p n'est pas un élément maximal de N, il existe $I_{p+1} \in E$ tel que $I_p \subsetneq I_{p+1}$. Par récurrence on a construit une suite d'idéaux de A strictement croissante, elle ne peut donc pas stationner. On en déduit que E admet un élément maximal pour l'inclusion.

(iii) $\implies$ (i) :
Considérons E l'ensemble des idéaux de A qui sont de type fini.
E n'est pas vide car l'idéal nul appartient à E par exemple. On sait donc que E possède un élément I maximal pour l'inclusion. Montrons que $A = I$.
On sait que I est de type fini donc il existe une famille fini $(a_i)_{i\in[\![1;q]\!]}$ qui engendre I. Supposons qu'il existe un élément $a \in A\backslash I$. Alors en posant $b_{q+1} = a$ et $\forall i \in [\![1;q]\!],\ b_i = a_i$, l'idéal J engendré par $(b_i)_{i\in[\![1;q+1]\!]}$ est un idéal de A de type fini. C'est donc un élément de E. Cependant I ne peut contenir J puisque $a \in J\backslash I$. Ceci contredit la maximalité de I dans E et on en déduit que $A = I$. Par conséquent que A est de type fini (en tant qu'idéal de lui-même).
Ainsi un idéal quelconque de A se doit d'être de type fini puisqu'il est contenu dans A.

2. La question précédente justifie immédiatement que tout anneau principal, où les idéaux sont engendrés par un seul élément, est noethérien et vérifie donc (ii). On sait ou on redémontre (cf. V.11) que $\mathbb{Z}$ est principal ce qui termine la question.
Toutefois on peut aussi le faire de manière directe : On se donne une suite croissante $(I_n)_{n\in\mathbb{N}}$ d'idéaux de $\mathbb{Z}$. On sait qu'il existe une suite $(N_n)_{n\in\mathbb{N}}$ d'entiers positifs tels que $\forall n \in \mathbb{N},\ I_n = N_n\mathbb{Z}$. Si la suite $(I_n)_{n\in\mathbb{N}}$ ne stationne pas à $\{0\}$ alors APCR $N_n > 0$.
Or $\forall n \in \mathbb{N},\ N_n\mathbb{Z} \subset N_{n+1}\mathbb{Z} \implies N_{n+1}|N_n$. Or comme APCR $N_n > 0$, la suite $(N_n)_{n\in\mathbb{N}}$ est une suite d'entiers positifs décroissante APCR. On montre alors classiquement qu'elle stationne et donc que $(I_n)_{n\in\mathbb{N}}$ stationne.

3. De même, le cours fournit que $\mathbb{K}[X]$ est principal ce qui, associé à la question 1, termine la question. Si l'on veut faire sans :
On se donne une suite croissante $(I_n)_{n\in\mathbb{N}}$ d'idéaux de $\mathbb{K}[X]$.

On sait qu'il existe une suite $(P_n)_{n\in\mathbb{N}}$ de $\mathbb{K}[X]$ telle que $\forall n \in \mathbb{N},\ I_n = P_n\mathbb{Z}$. Si la suite $(I_n)_{n\in\mathbb{N}}$ ne stationne pas à $\{0_{\mathbb{K}[X]}\}$ alors APCR $\deg(P_n) \geq 0$.
Or $\forall n \in \mathbb{N},\ (P_n\mathbb{K}[X] \subset P_{n+1}\mathbb{K}[X] \wedge P_n \neq 0_{\mathbb{K}[X]}) \implies P_{n+1}|P_n \implies \deg(P_{n+1}) \leq \deg(P_n)$. Or comme $\forall n \in \mathbb{N},\ \deg(P_n) \geq 0$, la suite $(\deg(P_n))_{n\in\mathbb{N}}$ est une suite d'entiers positifs décroissante. On montre alors classiquement qu'elle stationne. On sait alors que APCR P_n et P_{n+1} sont associés. Deux polynômes associés engendrant le même idéal, on en déduit que $(I_n)_{n\in\mathbb{N}}$ stationne.

XIII.6.13 Morphismes d'anneaux de fonctions réelles

[Enoncé]

XIII.6.14 Caractérisation d'un corps par ses idéaux ★★

[Enoncé]
Supposons que A est un corps. Soit I un idéal non nul de A.
Alors il existe $x \in \backslash\{0_A\}$. Comme A est un corps, x est inversible et par absorbance, $1_A = xx^{-1} \in I$. On en déduit encore par absorbance que $\forall a \in A,\ a = 1_A \times a \in I$. Ainsi $A = I$.
Réciproquement supposons que les seuls idéaux de A soient $\{0_A\}$ et A. Fixons $x \in A$ non nul et montrons qu'il est inversible.
On considère $I = \{xa,\ a \in A\}$. I est un idéal de A (c'est l'idéal engendré par x), on sait alors qu'il est soit nul soit égal à A.
Or il ne peut pas être nul car sinon comme $x \in I$, x serait nul. Donc $I = A$ et en particulier $1_A \in I$. C'est à dire qu'il existe $a \in A$ tel que $xa = 1_A$. Comme A est commutatif, cela montre que x est inversible d'inverse a.

XIII.6.15 Opérations sur les idéaux, idéaux principaux ★★★

[Enoncé]

1. Soient I et J deux idéaux de A.
   On sait (cf. V.6) que $I \cap J$ est un sous groupe de $(A, +)$. De plus, si $a \in A$ et $x \in I \cap J$ alors $ax \in I$ et $ax \in J$ par absorbance des idéaux I et J c'est à dire $ax \in I \cap J$. Ainsi $I \cap J$ est un idéal de A.
   Tout d'abord $I + J \subset A$ et $0_A = 0_A + 0_A$ et $0_A \in I$ et $0_A \in J$ donc $0_A \in I + J$.
   Ensuite si $x, y \in I + J$ alors $\exists (a, b), (c, d) \in I \times J,\ x = a + b,\ y = c + d$. Donc $x - y = a - c + b - d \in I + J$ car $a - c \in I$ et $b - d \in J$. Ainsi $I + J$ est un sous-groupe de $(A, +)$. Enfin, si $a \in A$ et $x \in I + J$ alors il existe $(i, j) \in I + J$ tel que $x = i + j$. Donc $ax = ai + aj \in I + J$ car $ai \in I$ et $aj \in J$ par absorbance. Ainsi $I + J$ est un idéal de A.
2. a. D'après le cours on sait que $a\mathbb{Z} + b\mathbb{Z} = \text{pgcd}(a, b)\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} = \text{ppcm}(a, b)\mathbb{Z}$.

b. Dans $\mathbb{Z}$ on sait qu'en écrivant $a = \text{pgcd}(a,b)u$ et $b = \text{pgcd}(a,b)v$ avec $u, v \in \mathbb{Z}$, alors comme $\text{ppcm}(a,b) \times \text{pgcd}(a,b) = |ab|$, on a $\text{ppcm}(a,b) = |\text{pgcd}(a,b)uv|$.
Soit $(a,b) \in A^2$. On suppose qu'il existe $d \in A$ tel que $aA + bA = dA$. $b \in dA$ et $a \in dA$ donc $\exists u, v \in A,\ a = du,\ b = dv$. En s'inspirant du résultat dans $\mathbb{Z}$ on pose $c = duv$. Montrons que $cA = aA \cap bA$.
$c = av = bu$ donc $c \in aA \cap bA$. Donc $cA \subset aA \cap bA$.
Réciproquement si $x \in aA \cap bA$ alors $\exists \alpha, \beta \in A,\ x = \alpha a = \beta b$. Par ailleurs il existe $\lambda, \mu \in A$ tels que $d = \lambda a + \mu b$.
Ainsi $x = \alpha a = \alpha u d = \alpha u(\lambda a + \mu b) = \lambda u x + \alpha\mu c = \lambda\beta u dv + \alpha\mu c = (\beta\lambda + \alpha\mu)c \in cA$. Donc $aA \cap bA \subset cA$ puis $aA + bA = cA$.

XIII.6.16 Idéal premier ★★

[Enoncé]
Soit $a \in A \backslash \{0_A\}$.
a^2A est un idéal de A et $a^2 = a \times a \in a^2A$ donc $a \in a^2A$.
Autrement dit $\exists b \in A,\ a = a^2b$ i.e $a(ab - 1_A) = 0_A$.
Or A est intègre, en effet $\{0_A\}$ est un idéal de A donc $\forall x, y \in A,\ xy = 0_A \implies (x = 0_A \text{ ou } y = 0_A)$.
Donc comme $a \neq 0_A$, $ab = 1_A$ c'est à dire a est inversible (d'inverse b).
Ainsi A est un corps.

XIII.6.17 Idéal maximal ★★★★

[Enoncé]

1. Soit I un idéal de A.
   Supposons que I est maximal et fixons $a \in A \backslash I$. $I + aA$ est un idéal de A qui contient I, il est donc égal à I ou à A. Or $a \in I + aA$ et $a \notin I$ donc $I + aA = A$.
   Réciproquement supposons que $\forall a \in A \backslash I,\ I + aA = A$ et fixons J un idéal de A qui contient strictement I.
   On sait qu'il existe $a \in J \backslash I$. Comme $a \in J,\ aA \subset J$. Par suite, $I + aA \subset J$. Enfin comme $a \notin I,\ I + aA = A$. Ainsi $J = A$ et I est maximal.
2. Soit I un idéal maximal de A. Fixons $a, b \in A \backslash I$.
   D'après la question précédente $I + aA = A = I + bA$. On sait alors qu'il existe $x \in I$ ainsi que $u \in A$ tel que $1_A = x + au$.
   Donc $b = bx + bau$. Si $ab \in I$ alors $bau \in I$. De plus $bx \in I$ car $x \in I$ donc $b \in I$ ce qui est absurde. Ainsi $ab \notin I$ et I est premier.
3. Dans n'importe quel anneau intègre, l'idéal nul est premier : cela veut exactement dire que l'anneau est intègre.
   Dans $\mathbb{Z}$, si p est un nombre premier alors $p\mathbb{Z}$ est premier : c'est le lemme d'Euclide. De plus ce sont les seuls idéaux premiers, en effet si a est un entier composée alors en écrivant

$a = bc$ avec $b \neq a$ et $c \neq a$ alors $b \notin a\mathbb{Z}$ et $c \notin a\mathbb{Z}$ pourtant $bc \in a\mathbb{Z}$.
Notons aussi que si p est premier alors $p\mathbb{Z}$ est maximal : $\forall a \notin p\mathbb{Z},\ a\mathbb{Z}+p\mathbb{Z} = \text{pgcd}(a,p)\mathbb{Z} = \mathbb{Z}$.

4. a. La fonction identiquement nulle s'annule en 0 et appartient donc à I. Fixons $(f,g,h) \in I^2 \times A$.
$(f-g)(0) = f(0) - g(0) = 0$ donc $f - g \in I$ et $(f \times h)(0) = f(0)h(0) = 0$ donc $f \times h \in I$.
Ainsi I est un idéal de A. Montrons qu'il est principal.
Soit $f \in I$. Montrons que $g : x \mapsto \begin{cases} \dfrac{f(x)}{x} & \text{si } x \neq 0 \\ f'(0) & \text{si } x = 0 \end{cases}$ est $\mathcal{C}^\infty$ sur $\mathbb{R}$.
$\forall x \in \mathbb{R}^*,\ f(x) = \displaystyle\int_0^x f'(t)dt = x\int_0^1 f'(ux)du$ c'est à dire $\forall x \in \mathbb{R}^*,\ g(x) = \displaystyle\int_0^1 f'(ux)du$. L'égalité est encore vraie pour $x = 0$.
De plus, $h : (u,x) \mapsto f'(ux)$ est de classe $\mathcal{C}^\infty$ sur $\mathbb{R} \times [0,1]$ par composition et pour tout $k \in \mathbb{N}$, $\dfrac{\partial^k h}{\partial x^k}(u,x) = u^k f^{(k+1)}(ux)$ est continue sur $\mathbb{R} \times [0,1]$. On peut donc dominer $u \mapsto \dfrac{\partial^k h}{\partial x^k}$ par $\varphi : u \mapsto \left\| u \mapsto \dfrac{\partial^k h}{\partial x^k} \right\|_{\infty,[a,b]}$ sur un segment $[a,b] \subset \mathbb{R}$.
Ainsi $g \in A$ par le théorème de transfert $\mathcal{C}^\infty$.
Donc $f = \text{Id}_{\mathbb{R}} \times g \in \text{Id}_{\mathbb{R}} A$.
Réciproquement $\text{Id}_{\mathbb{R}} \in I$ donc $\text{Id}_{\mathbb{R}} A \subset I$ d'où $I = \text{Id}_{\mathbb{R}} A$.
Montrons que I est maximal. Soient $f \notin I$ et $g \in A$.
$\forall x \in \mathbb{R},\ g(x) = \left(g(x) - \dfrac{g(0)}{f(0)}f(x)\right) + \dfrac{g(0)}{f(0)}f(x)$.
$h : x \in \mathbb{R} \mapsto g(x) - \dfrac{g(0)}{f(0)}f(x) \in I$ et $\dfrac{g(0)}{f(0)}f \in fA$ donc $g \in I + fA$.
Ainsi $I + fA = A$ et I est maximal. D'après la question précédente il est donc premier.

b. La fonction nulle est évidemment élément de J. Fixons $(f,g,h) \in J^2 \times A$.
$\forall k \in \mathbb{N},\ (f-g)^{(k)}(0) = f^{(k)}(0) - g^{(k)}(0) = 0$ donc $f - g \in J$ et d'après la formule de Leibniz,
$\forall k \in \mathbb{N},\ (f \times h)^{(k)}(0) = \displaystyle\sum_{i=0}^{k} \binom{k}{i} f^{(i)}(0)h^{(k-i)}(0) = 0$ donc $f \times h \in J$.
Ainsi J est un idéal de A. Il n'est pas maximal puisqu'il est contenu strictement dans I. Nonobstant il est premier : Si $f, g \notin I$ alors on note n l'entier tel que $f^{(n)}$ est la plus petite dérivée de f qui ne s'annule pas en 0. On note de même m pour g. $(f \times g)^{(m+n)}$ ne s'annule pas en 0 (il ne reste que le terme $f^{(n)}(0)g^{(m)}(0)$ qui est non nul).

Montrons par l'absurde que J n'est pas principal. On note f telle que $J = fA$.

Comme $f(0)=0$, d'après la question précédente il existe $g\in A$ telle que $f=\mathrm{Id}_{\mathbb{R}}\, g$.
Posons $\varphi : x\in\mathbb{R}\mapsto \begin{cases} e^{-1/x^2} & \text{si } x\neq 0\\ 0 & \text{si } x=0\end{cases}$. Il est classique de montrer que $\varphi\in J$:
On montre que les dérivés successives de φ s'exprime sous la forme d'une fraction rationnelle que multiplie e^{-1/x^2} et on utilise le théorème de la limite de la dérivée.
On peut donc trouver une fonction $h\in A$ telle que $\varphi=fh$. Comme φ ne s'annule qu'en 0, il en est de même pour f. Il en est donc de même pour tous les éléments de J.
On a montré dans la question précédente que $g=x\in\mathbb{R}\mapsto \displaystyle\int_0^1 f'(ux)du$ et que en particulier, $\forall k\in\mathbb{N},\ g^{(k)}(0)=\displaystyle\int_0^1 u^k f^{(k+1)}(0)du=0$. Ainsi $g\in J$.
On en déduit qu'il existe $h\in A$ telle que $g=fh=\mathrm{Id}_{\mathbb{R}}\, gh$. Or g ne s'annule qu'en 0 donc $\forall x\in\mathbb{R}^*,\ 1=xh(x)$. On obtient une absurdité en faisant tendre x vers 0.
Finalement J n'est pas principal.

XIII.6.18 Idéaux d'un espace de fonction

[Enoncé]

XIII.6.19 Radical d'un idéal ★

[Enoncé]

1. $(\forall x\in I,\ x^1\in I)\implies I\subset R(I)$. En particulier $0_A\in R(I)$. $R(I)$ est clairement inclus dans A. Soient $x,y\in R(I)$.
   A étant commutatif, $\forall p\in\mathbb{N},\ (x-y)^p=\displaystyle\sum_{k=0}^{p}\binom{p}{k}x^k(-y)^{p-k}$.
   On sait qu'il existe deux entiers naturels n et m tels que $x^n\in I$ et $y^m\in I$. Posons $p=n+m$.
   Si $n\leq k\leq p$ alors $\displaystyle\binom{p}{k}x^k(-y)^{p-k}=x^n\times\binom{p}{k}x^{k-n}(-y)^{p-k}\in I$ par absorbance.
   Et si $0\leq k\leq n-1$ alors $m+1\leq p-k$ donc $\displaystyle\binom{p}{k}x^k(-y)^{p-k}=y^m\times(-1)^{p-k}\binom{p}{k}x^k y^{p-k-m}\in I$ par absorbance.
   Finalement $(x-y)^p\in I$ car I est stable par somme.
   De plus, $\forall a\in A,\ (ax)^n=a^n x^n\in I$ par absorbance.
   Ainsi $R(I)$ est un idéal de A.
2. D'après la question précédente on a déjà $R(I)\subset R(R(I))$.
   Fixons $x\in R(R(I))$. On sait qu'il existe $n\in\mathbb{N}$ tel que $x^n\in R(I)$. Donc on sait qu'il existe $m\in\mathbb{N},\ (x^n)^m=x^{nm}\in I$. $nm\in\mathbb{N}$ donc $x\in R(I)$.
   Ainsi $R(R(I))=R(I)$.

3. Il est évident que si $E \subset F$ sont deux idéaux de A alors $R(E) \subset R(F)$. $I \cap J \subset I$ et $I \cap J \subset J$ donc $R(I \cap J) \subset R(I)$ et $R(I \cap J) \subset R(J)$. Par conséquent $R(I \cap J) \subset R(I) \cap R(J)$.
Réciproquement donnons nous $x \in R(I) \cap R(J)$. On sait qu'il existe deux entiers naturels n et m tels que $x^n \in I$ et $x^m \in I$. Posons $p = \max(n, m) \in \mathbb{N}$. $x^p = x^n x^{p-n} = x^m x^{p-m} \in I \cap J$ donc $x \in R(I \cap J)$.
Ainsi $R(I \cap J) = R(I) \cap R(J)$.

XIII.6.20 Nilradical ★★

[Enoncé]

1. Tout d'abord, $\mathcal{N}(A) \subset A$ et $0_A = 0_A^1 \in \mathcal{N}(A)$. Fixons $(x, y, a) \in \mathcal{N}(A)^2 \times A$.
A étant commutatif, $\forall p \in \mathbb{N},\ (x-y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k (-y)^{p-k}$.
On sait qu'il existe deux entiers naturels n et m tels que $x^n \in I$ et $y^m \in I$. Posons $p = n + m$.
Si $n \leq k \leq p$ alors $\binom{p}{k} x^k (-y)^{p-k} = x^n \times \binom{p}{k} x^{k-n} (-y)^{p-k} = 0_A$.
Et si $0 \leq k \leq n-1$ alors $m+1 \leq p-k$ donc $\binom{p}{k} x^k (-y)^{p-k} = y^m \times (-1)^{p-k} \binom{p}{k} x^k y^{p-k-m} = 0_A$.
Finalement $(x-y)^p \in I$ car I est stable par somme.
De plus, $(ax)^n = a^n x^n = 0_A$.
Ainsi $\mathcal{N}(A)$ est un idéal de A.
Remarque : C'est le radical de l'idéal nul, $\mathcal{N}(A) = R(\{0_A\})$.
2. Soit $\overline{k}$ un élément nilpotent de $\mathbb{Z}/n\mathbb{Z}$ (on prend k entre 0 et $n-1$). On note $m \in \mathbb{N}^*$ tel que $\overline{k}^p = \overline{k^m} = \overline{0}$, i.e $n | k^m$.
Notons p un diviseur premier. $p|n|k^m$ donc $p|k^m$. D'après le lemme d'Euclide, $p|k$. Ainsi k doit admettre au moins tous les diviseurs premiers de n comme diviseurs.
Réciproquement si quel que soit p premier, $p|n \implies p|k$ alors en notant m la valuation p-adique de n maximale, on peut affirmer que quel que soit p un diviseur premier de n, $v_p(k) \geq 1$ d'où $v_p(n) \leq m \leq m v_p(k) = v_p(k^m)$. Donc $n|k^m$ c'est à dire $\overline{k}^m = \overline{0}$, c'est à dire $\overline{k} \in \mathcal{N}(\mathbb{Z}/n\mathbb{Z})$.
Finalement, $\mathcal{N}(\mathbb{Z}/n\mathbb{Z}) = \{\overline{k} \mid k \in [\![0; n-1]\!],\ \forall p \in \mathbb{P},\ p|n \implies p|k\}$.

XIII.6.21 Radical de Jacobson ★★

[Enoncé]

1. Soit I un idéal de A.
Supposons que I est maximal et fixons $a \in A \backslash I$. $I + aA$ est un idéal de A qui contient I, il est donc égal à I ou à A. Or $a \in I + aA$ et $a \notin I$ donc $I + aA = A$.

Réciproquement supposons que $\forall a \in A \backslash I,\ I + aA = A$ et fixons J un idéal de A qui contient strictement I.
On sait qu'il existe $a \in J \backslash I$. Comme $a \in J,\ aA \subset J$. Par suite, $I + aA \subset J$. Enfin comme $a \notin I,\ I + aA = A$. Ainsi $J = A$ et I est maximal.

2. Soit $x \in A$.
Supposons que $x \notin J$. On sait qu'il existe un idéal maximal I de A pour lequel $x \notin I$.
Donc d'après la question 1, $I + xA = A$. En particulier $1_A \in I + xA$ i.e $\exists (y, a) \in I \times A,\ 1_A = y + ax$. Donc $1_A - ax = y \in I$. Or $I \neq A$ puisqu'il est maximal. Par conséquent tous ses éléments sont non inversibles, puisque sinon on aurait $1_A \in I$ par absorbance puis $I = A$ encore par absorbance. Ainsi $1_A - ax \notin A^\times$.

Réciproquement supposons qu'il existe $a \in A$ tel que $y = 1_A + ax \notin A^\times$.
On sait alors que $yA \neq A$. D'après le théorème admis on peut l'inclure dans un idéal maximal I. Supposons par l'absurde que $x \in I$.
Alors $ax \in I$ par absorbance et comme $y \in I$ par définition de I on obtient que $1_A \in I$ d'où $I = A$ ce qui est absurde.
Ainsi $x \notin I$ et par suite, $x \notin J$.

Remarque : Le théorème de Krull est en fait équivalent à l'axiome du choix

XIII.6.22 Idéaux de $\mathcal{M}_n(\mathbb{K})$

[Enoncé]

Idéaux bilatère

Idéaux à droite

Idéaux à gauche

XIII.6.23 Caractéristique d'un anneau

[Enoncé]

1. — $\phi(1) = 1.1_A = 1_A$.
— Soit $(k, l) \in \mathbb{Z}^2$. $\varphi(k + l) = (k + l)1_A = k1_A + l1_A = \varphi(k) + \varphi(l)$.
— Soit $(k, l) \in \mathbb{Z}^2$. $\varphi(kl) = (kl)1_A = k1_A \circ l1_A = \varphi(k) \circ \varphi(l)$.
Donc φ est un morphisme d'anneaux.
2. On sait que le noyau de φ est un sous-groupe de $(\mathbb{Z}, +)$. Or les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$. V.11.
Donc il existe $n \in \mathbb{N}$ tel que $\mathrm{Ker}(\varphi) = n\mathbb{Z}$.
3. Supposons que A est un anneau intègre.
On note n la caractéristique de A.

Si $n = 0$, on a terminé.
Si $n > 0$, montrons que n est premier. Supposons que n n'est pas premier. Il existe $(a, b) \in \mathbb{Z}^2$ tel que $n = ab$.
On a $(a1_A)(b1_B) = (ab)1_A = n1_A = 0$.
Puisque A est un anneau intègre, on en déduit que a ou b est nul.
Ce qui contredit le fait que $n > 0$, ce qui est absurde.
Donc n est premier.

4. On sait qu'un corps est un anneau intègre, donc d'après la question précédent, K est de caractéristique nulle ou égale à un nombre premier.
Supposons que p est nulle.
Cela signifie que $\forall k \in \mathbb{Z}^*, k1_K \neq O_K$.
Ainsi, on en déduit que $\forall (k, j) \in \mathbb{N}^*, k1_K \neq j1_K$, ce qui est absurde car K est fini. Donc p est un nombre premier.
On sait que $(K, +, \times)$ est un corps, il suffit donc de munir K d'une loi de composition externe $*$.
$\forall \lambda \in \mathbb{Z}/p\mathbb{Z}, \exists k \in \mathbb{Z}$ tel que $\lambda = \overline{k}$. On pose :

$$f : \left\{ \begin{array}{rcl} \mathbb{Z}/p\mathbb{Z} \times K & \longrightarrow & K \\ (\lambda, x) & \longmapsto & kx \end{array} \right.$$

Montrons que f est bien définie.
$\forall (k, k') \in \mathbb{Z}$ tel que $\overline{k} = \overline{k'}$.
Il existe $l \in \mathbb{Z}$, tel que $k' = k + lp$.

$$\forall x \in K, k'x = kx + lpx = kx$$

car K est de caractéristique p.
Il suffit maintenant de vérifier que :

- Pour tout $x \in K$, $f((\overline{1}, x)) = x$
- Pour tous $(\overline{k}, \overline{l}) \in (\mathbb{Z}/p\mathbb{Z})^2, x \in K$, $f((\overline{k+l}, x)) = f(\overline{k}, x) + f(\overline{l}, x)$
- Pour tous $(\overline{k}, \overline{l}) \in (\mathbb{Z}/p\mathbb{Z})^2, x \in K$, $f((\overline{kl}, x)) = f(\overline{k}, x) \times f(\overline{l}, x)$
- Pour tous $\overline{k} \in \mathbb{Z}/p\mathbb{Z}, (x_1, x_2) \in K^2$, $f((\overline{k}, x_1 + x_2)) = f((\overline{k}, x_1)) + f((\overline{k}, x_2))$

Par conséquent, K est alors un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension finie.
Soit $(e_1, \ldots, e_n)$ une base de K.
On pose :

$$f : \left\{ \begin{array}{rcl} (\mathbb{Z}/p\mathbb{Z})^n & \longrightarrow & K \\ (\lambda_1, \ldots, \lambda_n) & \longmapsto & \displaystyle\sum_{k=1}^{n} \lambda_k e_k \end{array} \right.$$

Cette application est bien évidemment un isomorphisme.
Par conséquent,

$$\mathrm{Card}(K) = p^n$$

XIII.6.24 Anneau intègre ★★

[Enoncé]

1. Soit $(K,+,\times)$ un corps et soient $x \in K\backslash\{0\},\ y \in K$.
   Si $xy = 0_K$ alors en multipliant par x^{-1} à gauche on a $y = 0_K$.
   Ainsi K est intègre.
2. L'anneau des nombres décimaux est intègre en tant que sous-anneau de $\mathbb{C}$ qui l'est. Pourtant ce n'est pas un corps car par exemple 3 n'admet pas d'inverse dans $\mathbb{D}$. De même pour l'anneau des entiers relatifs $\mathbb{Z}$.
3. Tout d'abord $A[X]$ est un anneau commutatif.

   Supposons que A est intègre. Soient $P,Q \in A[X]\backslash\{0\}$. On écrit $P = \sum_{n=0}^{+\infty} a_n X^n$ et $Q = \sum_{n=0}^{+\infty} b_n X^n$.

   Alors $PQ = \sum_{n=0}^{+\infty}\left(\sum_{k=0}^{n} a_k b_{n-k}\right) X^n = \sum_{n=0}^{+\infty} c_n X^n$. Notons i l'indice du premier coefficient non nul de P et j l'indice du premier coefficient non nul de Q. On sait qu'ils en ont au moins un puisqu'ils sont non nuls.
   Alors $c_{i+j} = a_i b_j \neq 0$ d'où $PQ \neq 0$ et $A[X]$ est intègre.
   Réciproquement, si $A[X]$ est intègre alors :

   $$\forall x,y \in A,\ xy = 0_A \implies x1_{A[X]} \times y1_{A[X]} = 0_{A[X]} \implies x1_{A[X]} = 0_{A[X]} \vee y1_{A[X]} = 0_{A[X]} \implies x = 0$$

   Donc A est intègre.

XIII.6.25 Sous-corps minimal de $\mathbb{C}$ ★

[Enoncé]
Soit K un sous-corps de $\mathbb{C}$. On a $0,1 \in K$.
Par somme et passage à l'opposé on a donc $\mathbb{Z} \subset K$. Puis par quotient, $\mathbb{Q} \subset K$.
$\mathbb{Q}$ est un sous-corps de $\mathbb{C}$, c'est donc le sous-corps minimal de $\mathbb{C}$ au sens de l'inclusion.

XIII.6.26 Corps d'Attila

[Enoncé]

1. $(Vect(A),+)$ est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{K})$ donc $(Vect(A),+)$ est un groupe abélien.
   Par associativité et distributivité du produit de $\mathbb{K}$, on en déduit que $\times$ est associative

et distributive par rapport à $+$.
On cherche maintenant le neutre de cette loi i.e. on cherche $\lambda \in \mathbb{K}$ tel que

$$\forall \mu \in \mathbb{K}, \lambda A \mu A = \mu A$$

Soit $\mu \in \mathbb{K}$. On remarque que $A^2 = nA$ ainsi :

$$\lambda \mu n A = \lambda \mu A^2 = \mu A$$

Donc $\lambda n = 1$ i.e.

$$\lambda = \frac{1}{n}$$

Donc, le neutre pour cette loi est $\frac{1}{n}A$.

Remarque : le neutre ici n'est pas I_n. On vérifie que l'inverse de μA est $\frac{1}{\mu n}A$.

2. D'après ce qui précède, $(\text{Vect}(A) \setminus 0, \times)$ est un groupe de neutre $\frac{1}{n}A$.

XIII.6.27 Endomorphisme de corps de $\mathbb{R}$ ★★

[Enoncé]

1. On sait que $f(0) = 0$ et $f(1) = 1$ donc par récurrence immédiate à l'aide de la relation $f(x+y) = f(x) + f(y)$, $\forall n \in \mathbb{N},\ f(n) = n$. Donc $\forall n \in \mathbb{N},\ 0 = f(0) = f(n-n) = f(n) - f(n)$ d'où $\forall k \in \mathbb{Z},\ f(k) = k$.
Fixons $x = \frac{p}{q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$.
On a $qf(x) = f(qx) = f(p) = p$. Donc $f(x) = \frac{p}{q} = x$.
Ainsi $f_{|\mathbb{Q}} = \text{Id}_{\mathbb{Q}}$.
2. Soit $z \geq 0$. $f(z) = f(\sqrt{z}^2) = f(\sqrt{z})^2 \geq 0$.
Soient $x, y \in \mathbb{R}$ $x \geq y$.
$f(x) - f(y) = f(x-y) \geq 0$ car $x - y \geq 0$. Ainsi f est croissante sur $\mathbb{R}$.
3. Soient $x \in \mathbb{R}$. Supposons que $f(x) \neq x$.
Si $f(x) > x$ alors par densité de $\mathbb{Q}$ dans $\mathbb{R}$, $\exists t \in \mathbb{Q},\ f(x) > t > x$.
Alors $f(x) - t = f(x) - f(t) = f(x-t) \geq 0$ d'où $x - t \geq 0$ par croissance de f. Ceci est absurde donc $f(x) < x$. Mais alors par densité de $\mathbb{Q}$ dans $\mathbb{R}$, $\exists u \in \mathbb{Q},\ f(x) < u < x$. De même on obtient $x - u < 0$ ce qui est absurde.
On en déduit que $f(x) = x$ et $f = \text{Id}_{\mathbb{R}}$.

XIII.6.28 Automorphismes de $\mathbb{Q}[\sqrt{2}]$ ★★★

[Enoncé]

L'application $\Phi : \left\{ \begin{array}{ccc} \mathbb{Q}_1[X] & \longrightarrow & \mathbb{Q}[\sqrt{2}] \\ P & \longmapsto & P(\sqrt{2}) \end{array} \right.$ est un morphisme d'algèbre.

Donc $\mathbb{Q}[\sqrt{2}]$ est une sous-algèbre de $\mathbb{C}$ et en particulier un sous-anneau de $\mathbb{C}$.
De plus, si $a+b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]\backslash\{0\}$ alors $\dfrac{1}{a+b\sqrt{2}} = \dfrac{a-b\sqrt{2}}{a^2-2b^2} = c+d\sqrt{2}$ avec $c = \dfrac{a}{a^2-2b^2} \in \mathbb{Q}$ et $d = -\dfrac{b}{a^2-2b^2} \in \mathbb{Q}$.
Donc $\dfrac{1}{a+b\sqrt{2}} \in \mathbb{Q}[\sqrt{2}]$ c'est à dire $\mathbb{Q}[\sqrt{2}]$ est un sous-corps de $\mathbb{C}$.
Donnons nous f un automorphisme de $\mathbb{Q}[\sqrt{2}]$.
On remarque que $f(\sqrt{2})^2 = f(\sqrt{2}^2) = f(2) = 2f(1) = 2$.
Donc $f(\sqrt{2}) = \varepsilon\sqrt{2}$ avec $\varepsilon \in \{-1, 1\}$.
Ensuite, on sait que $f(0) = 0$ et $f(1) = 1$ donc par récurrence immédiate à l'aide de la relation $f(x+y) = f(x)+f(y)$, $\forall n \in \mathbb{N},\ f(n) = n$. Donc $\forall n \in \mathbb{N},\ 0 = f(0) = f(n-n) = f(n)-f(n)$ d'où $\forall k \in \mathbb{Z},\ f(k) = k$.
Fixons $x = \dfrac{p}{q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$.
On a $qf(x) = f(qx) = f(p) = p$. Donc $f(x) = \dfrac{p}{q} = x$.
Ainsi si $z = a+b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ alors $f(x) = f(a)+f(b)f(\sqrt{2}) = a+\varepsilon b\sqrt{2}$.
On vérifie que si $\varepsilon \in \{-1,1\}$, $f_\varepsilon : \begin{cases} \mathbb{Q}[\sqrt{2}] & \longrightarrow & \mathbb{Q}[\sqrt{2}] \\ a+b\sqrt{2} & \longmapsto & a+\varepsilon b\sqrt{2} \end{cases}$ est un automorphisme de $\mathbb{Q}[\sqrt{2}]$. Ce sont dont les seuls automorphismes de $\mathbb{Q}[\sqrt{2}]$.

XIII.6.29 Algèbre des quaternions

[Enoncé]

XIII.6.30 Une définition de $\mathbb{C}$ ★★

[Enoncé]

1. Soient $z = a+ib$ et $z' = a'+b'i$ des complexes. Soit $\lambda \in \mathbb{R}$.
   $\Phi(z+\lambda z') = \begin{pmatrix} a+\lambda a' & -(b+\lambda b') \\ b+\lambda b' & a+\lambda a' \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \lambda \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} = \Phi(z) + \lambda\Phi(z')$,
   et $\Phi(zz') = \begin{pmatrix} aa'-bb' & -(ab'+a'b) \\ ab'+a'b & aa'-bb' \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \times \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} = \Phi(z)\Phi(z')$.
   Donc Φ est un morphisme de $\mathbb{R}$-algèbres.
   De plus, si $z \in \mathbb{C}$ tel que $\Phi(z) = I_2$ alors $\Re(z) = 1$ et $\Im(z) = 0$ c'est à dire $z = 1$. Donc Φ est injective.
2. Fixons $\theta \in \mathbb{R}$. $A_\theta = \Phi(i\theta)$.
   Φ étant linéaire sur $\mathbb{C}$ vu comme un $\mathbb{R}$-espace vectoriel de dimension finie, elle est continue.
   De plus, comme Φ est un morphisme d'algèbre, $\forall P \in \mathbb{R}[X],\ \Phi(P(z)) = P(\Phi(z))$. Ainsi

$\forall n \in \mathbb{N},\ \sum_{k=0}^{n} \frac{A_\theta^k}{k!} = \Phi\left(\sum_{k=0}^{n} \frac{(i\theta)^k}{k!}\right)$.

On sait que $\sum_{k=0}^{+\infty} \frac{(i\theta)^k}{k!} \underset{n\to+\infty}{\longrightarrow} e^{i\theta}$ et $\sum_{k=0}^{+\infty} \frac{A_\theta^k}{k!} \underset{n\to+\infty}{\longrightarrow} \exp(A_\theta)$.

Donc par continuité de Φ, $\exp(A_\theta) = \Phi(e^{i\theta}) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$.

XIII.6.31 $\mathbb{R}$-algèbre commutative intègre de dimension finie ★★★★

[Enoncé]

1. $\forall x, y \in \mathbb{K},\ \forall \lambda \in \mathbb{R},\ f(x+\lambda y) = a(x+y) = ax + \lambda ay = f(x) + \lambda f(y)$.
   De plus, si $z \in \mathbb{K}$ tel que $f(z) = 0$ alors $az = 0$ d'où $z = 0$ par intégrité de $\mathbb{K}$, vu que a n'est pas nul. Donc f est un endomorphisme injectif de l'espace vectoriel $\mathbb{K}$ de dimension fini, c'est donc un automorphisme de $\mathbb{K}$. On en déduit qu'il existe $x \in \mathbb{K},\ ax = 1$. Autrement dit a est inversible d'inverse x.
2. Soient $\lambda, \mu \in \mathbb{R}$ tels que $\lambda + \mu a = 0$. Si $\mu \neq 0$ alors $a = -\frac{\lambda}{\mu} \in \mathbb{R}$ ce qui est absurde. Donc $\mu = 0$ et par suite $\lambda = 0$. Par conséquent $(1, a)$ est libre dans $\mathbb{K}$.
   Ensuite, comme la famille $(1, a, \dots, a^n)$ est liée dans $\mathbb{K}$, a admet un polynôme annulateur P à coefficients réels.
   On écrit sa décomposition en produit de polynômes irréductibles dans $\mathbb{R}[X]$, $P = \prod_{i=1}^{r} P_i$.
   On sait que a est racine d'au moins un des P_i. Sans perte de généralité on suppose que c'est P_1.
   P_1 est irréductible dans $\mathbb{R}[X]$, il est donc de degré au plus 2. Autrement dit en écrivant $P_1 = \alpha + \beta X + \gamma X^2$ on a $\alpha + \beta a + \gamma a^2 = 0$ et $(1, a, a^2)$ est liée dans $\mathbb{K}$.
3. Comme $\mathbb{K}$ est dimension supérieure à 2 on sait qu'il existe $a \in \mathbb{K}\backslash\mathbb{R}$. D'après la question 2 on peut écrire $\alpha + \beta a + a^2 = 0$ avec $(\alpha, \beta) \in \mathbb{R}^2$.
   Ainsi $\left(a + \frac{\beta}{2}\right)^2 + \alpha - \frac{\beta^2}{4} = 0$. On pose alors $i = \frac{2}{\sqrt{4\alpha - \beta^2}}\left(a + \frac{\beta}{2}\right)$.
   La quantité $4\alpha - \beta^2$ est bien positive puisque c'est l'opposé du déterminant du polynôme $X^2 + \beta X + \alpha \in \mathbb{R}[X]$ dont on sait qu'il n'a pas de racines réelles (a est une racine non réelle et la somme des racines vaut $-\beta \in \mathbb{R}$).
   i est évidemment non réel donc la famille $(1, i)$ est libre dans $\mathbb{K}$. Montrons qu'elle est génératrice.
   Soit $a \in \mathbb{K}$. Si $a \in \mathbb{R}$ alors $a = a + 0 \cdot i \in \mathrm{Vect}(1, i)$. Et si $a \in \mathbb{K}\backslash\mathbb{R}$ alors $(1, a)$ est libre et $(1, a, a^2)$ est liée. Or d'après ce qui a été fait précédemment on peut écrire $i = \frac{2}{\sqrt{4\alpha - \beta^2}}\left(a + \frac{\beta}{2}\right)$ pour de certains réels α, β.
   Mais alors $a = \frac{\sqrt{4\alpha - \beta^2}}{2} i - \frac{\beta}{2} \in \mathrm{Vect}(1, i)$.

Finalement, $(1, i)$ est une base de $\mathbb{K}$ et donc $\mathbb{K}$ est de dimension 2. On sait donc que $\mathbb{K}$ est isomorphe à $\mathbb{C}$ en tant que $\mathbb{R}$-algèbre.

XIII.6.32 Théorie algébrique des corps ★★★★

[Enoncé]

1. cf. VI.9.
2. Montrons que l'ensemble $I_a = \{P \in \mathbb{K}[X],\ P(a) = 0\}$ est un idéal non nul de $\mathbb{K}[X]$. Déjà I_a est non nul car a est algébrique sur $\mathbb{K}$. Fixons $P, Q \in I_a$ et $R \in \mathbb{K}[X]$.
   $(P-Q)(a) = P(a) - Q(a) = 0$ et $(RP)(a) = R(a)P(a) = 0$ donc I_a est un idéal de $\mathbb{K}[X]$.
   On sait d'après la question précédente qu'il existe un polynôme P qui l'engendre.
   On pose μ le polynôme P divisé par son coefficient dominant. μ et P sont associés, ils engendrent donc le même idéal.
   Ainsi $\mu\mathbb{K}[X] = I_a$ c'est à dire $\forall Q \in \mathbb{K}[X],\ Q(a) = 0 \implies Q \in I_a \implies \mu | Q$.
   Supposons qu'il existe un autre polynôme T unitaire tel que $I_a = T\mathbb{K}[X]$. Alors comme $\mu \in I_a,\ T|\mu$ et comme $T \in I_a,\ \mu|T$. μ et T étant tout deux unitaires il suit que $T = \mu$.
   Vérifions maintenant que μ est irréductible. Soient $A, B \in \mathbb{K}[X]$ tels que $\mu = AB$.
   Alors $\mu(a) = 0 = A(a)B(a)$. $\mathbb{K}$ étant un corps, il est intègre d'où $A(a) = 0$ ou $B(a) = 0$.
   Donc $\mu|A$ ou $\mu|B$. Or A et B sont de degrés au plus $\deg \mu$. On en déduit que $A = \mu$ ou $B = \mu$ et donc que μ est irréductible.
   Ensuite montrons que $\mathcal{F} = (1, a, \dots, a^{\deg \mu - 1})$ est une base de $\mathbb{K}[a]$. Soit $P \in \mathbb{K}[X]$. On écrit $P = Q\mu + R$ une division euclidienne de P par μ. On a $P(a) = Q(a)\mu(a) + R(a) = R(a)$ avec $\deg R \leq \deg \mu - 1$. Ainsi $\mathbb{K}[X] = \text{Vect}(\mathcal{F})$.
   D'autre part, si $T \in \mathbb{K}[X]$ est de degré inférieur à $\deg \mu - 1$ annule a alors par définition de μ, $\mu|T$. Ceci n'est possible que si $T \in \mathbb{K}[X]$ est nul. On a montré que la seule combinaison d'éléments de $\mathcal{F}$ à coefficients dans $\mathbb{K}$ qui est nulle est la combinaison nulle, c'est à dire que $\mathcal{F}$ est libre.
   Ainsi $\mathcal{F}$ est une base de $\mathbb{K}[a]$ et $\mathbb{K}[a]$ est un $\mathbb{K}$-espace vectoriel de dimension $\deg \mu$.
   Montrons que $\mathbb{K}[a]$ est un sous-corps de $\mathbb{L}$. Tout d'abord $0_{\mathbb{K}[X]}(a) = 0 \in \mathbb{K}[a]$ et $1_{\mathbb{K}[X]}(a) = 1 \in \mathbb{K}[a]$. Fixons $(P, Q) \in \mathbb{K}[X]^2$.
   $P - Q \in \mathbb{K}[X]$ donc $P(a) - Q(a) = (P-Q)(a) \in \mathbb{K}[a]$. De même, $P(a)Q(a) = (PQ)(a) \in \mathbb{K}[a]$.
   Supposons que $P(a) \neq 0$. P n'est donc pas un multiple de μ et comme μ est irréductible, P et μ sont premiers entre eux.
   Donc d'après le théorème de Bézout il existe $U, V \in \mathbb{K}[X]$ tels que $PU + \mu V = 1$. Et en évaluant en 1, $P(a)U(a) = 1$ c'est à dire $P(a)^{-1} = U(a) \in \mathbb{K}[a]$.
   Par conséquent $\mathbb{K}[a]$ est un sous-corps de $\mathbb{L}$.
3. Il s'agit de trouver un polynôme à coefficients rationnels qui annule a.
   On remarque que $(a - \sqrt{2})^3 = 2$ ce qui donne en développant $a^3 + 6a - 2 = \sqrt{2}(3a^2 + 2)$ puis en élevant au carré :

$$a^6 - 6a^4 - 4a^3 + 12a^2 - 24a - 4 = 0$$

On a montré que a est algébrique (en fait c'est même un *entier algébrique* puisque le polynôme annulateur est unitaire à coefficients entiers). On sait que son polynôme minimal μ est un diviseur de $P = X^6 - 6X^4 - 4X^3 + 12X^2 - 24X - 4$.
Considérons maintenant le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[a]$. D'après la question précédente il est de dimension $\deg \mu$.
On remarque que la relation $a^3 + 6a - 2 = \sqrt{2}(3a^2 + 2)$ montre que $\sqrt{2} \in \mathbb{Q}[a]$, en effet $\mathbb{Q}[a]$ est un corps, $3a^2 + 2 > 0$ donc $\sqrt{2} = (a^3 + 6a - 2)(3a^3 + 6a - 2)^{-1} \in \mathbb{Q}[a]$.
On en déduit de plus que $\sqrt[3]{2} = a - \sqrt{2} \in \mathbb{Q}[a]$. Enfin comme $\mathbb{Q}[a]$ est une $\mathbb{Q}$-algèbre, $\forall P \in \mathbb{Q}[X],\ P(\sqrt{2}) \in \mathbb{Q}[a]$ et $P(\sqrt[3]{2}) \in \mathbb{Q}[a]$. On a donc les inclusions :

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[a] \text{ et } \mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{Q}[a]$$

Or le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$ est $X^2 - 1$ et celui de $\sqrt[3]{2}$ est $X^3 - 2$, cela découle du fait qu'ils n'ont pas de racine rationnelle.
La relation du multiplicité des degrés donne alors $2|\deg \mu$ et $3|\deg \mu$. Ainsi $6|\deg \mu$ d'où $6 \leq \deg \mu$. Or $\mu | P$ donc $\deg \mu = 6$.
On en déduit que $\deg \mu = 6$ et comme il est unitaire, $\mu = P$.

XIII.6.33 Famille $\mathbb{Q}$-libre ★★★★

[Enoncé]

1. Notons $\mathbb{Q}[\alpha] = \{P(\alpha),\ P \in \mathbb{Q}[X]\}$. Montrons que $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$. Dans un premier temps on montre (cf. VI.32) que $\mathbb{Q}[\alpha]$ est un sous-corps de $\mathbb{C}$ qui contient $\mathbb{Q}$ et α. Dans un second temps, si K est un corps qui contient $\mathbb{Q}$ et α alors il contient tous les polynômes en α à coefficients rationnels, c'est à dire $\mathbb{Q}[\alpha]$. Donc $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$. On montre ensuite (cf. VI.32) que $(1, \alpha, \dots, \alpha^{\deg \pi_\alpha - 1})$ est une base de $\mathbb{Q}[\alpha]$. Donc $\mathbb{Q}(\alpha)$ est un $\mathbb{Q}$-espace vectoriel de dimension $\deg \pi_\alpha$.
   Enfin, montrons que m_α est un endomorphisme de $\mathbb{Q}(\alpha)$.
   $\forall x \in \mathbb{Q}(\alpha),\ \alpha \in \mathbb{Q}(\alpha) \implies m_\alpha(x) = \alpha x \in \mathbb{Q}(\alpha)$. De plus, $\forall x, y \in \mathbb{Q}(\alpha),\ \forall \lambda \in \mathbb{Q},\ m_\alpha(x + \lambda y) = \alpha x + \lambda \alpha y = m_\alpha(x) + \lambda m_\alpha(y)$.
   Remarque : L'égalité $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$ n'est vraie que si α est un nombre algébrique. Par exemple pour π, $\frac{1}{\pi} \in \mathbb{Q}(\pi)$ puisque $\mathbb{Q}(\pi)$ est un corps. Or si il existait un polynôme $P \in \mathbb{Q}[X]$ tel que $P(\pi) = \frac{1}{\pi}$ alors le polynôme $Q = XP - 1 \in \mathbb{Q}[X]$ annulerait π. Or il est bien connu que π est un nombre transcendant et donc que ceci n'est pas possible.
2. Le polynôme $X^2 - d$ annule $\sqrt{d}$ donc $\sqrt{d}$ est algébrique. Déterminons son polynôme minimal.
   On sait que $\pi_{\sqrt{d}} | X^2 - d$. Si $\pi_{\sqrt{d}}$ était de degré 1 alors on aurait $\pi_{\sqrt{d}} = X - \sqrt{d}$.
   Or $\sqrt{d} \notin \mathbb{Q}$. En effet, supposons que $\sqrt{d} = \frac{a}{b}$ avec $a, b \in \mathbb{N}^*$ premiers entre eux. Alors $db^2 = a^2$.
   Montrons qu'un entier positif est le carré d'un entier non nul si et seulement si toutes

ses valuations p-adique sont paires. Soit $m \in \mathbb{N}^*$. Si $m = 1$ alors toutes ses valuation p-adique sont nulles donc c'est bon. Supposons que $m = k^2$ pour un certain $k \geq 2$. On sait que $m = \prod_{p \text{ premier}} p^{v_p(m)} = \left(\prod_{p \text{ premier}} p^{v_p(k)} \right)^2 = \prod_{p \text{ premier}} p^{2v_p(k)}$. Donc par unicité de la décomposition en facteurs premiers, quel que soit p premier $v_p(m) = 2v_p(k)$.
Réciproquement si quel que soit p premier il existe $k_p \in \mathbb{N}$ tel que $v_p(m) = 2k_p$, alors $m = k^2$ avec $k = \prod_{p \text{ premier}} p^{k_p} \in \mathbb{N}^*$.
On en déduit que d a un diviseur premier p pour lequel $v_p(d)$ est impair. De plus on sait que $v_p(a^2)$ et $v_p(b^2)$ sont pairs. Mais alors l'égalité $db^2 = a^2$ qui donne $v_p(d) + v_p(b^2) = v_p(a^2)$ est absurde. Ainsi $\sqrt{d} \notin \mathbb{Q}$.
Par conséquent π_α est de degré au moins 2 et par suite comme il est unitaire, $\pi_\alpha = X^2 - d$. Alors d'après la question précédente $\mathbb{Q}(\sqrt{d})$ est un $\mathbb{Q}$-espace vectoriel de dimension 2 dont une base est $(1, \sqrt{d})$. Autrement dit $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d},\ (a, b) \in \mathbb{Q}^2\}$.

3. Il est clair que $\forall k \in \mathbb{N},\ \forall x \in \mathbb{Q}(\alpha),\ m_\alpha^k(x) = \alpha^k x$. Donc par linéarité, $\forall P \in \mathbb{Q}[X],\ \forall x \in \mathbb{Q}(\alpha),\ P(m_\alpha)(x) = P(\alpha)x$. Ainsi $\forall P \in \mathbb{Q}[X],\ P(m_\alpha) = 0 \iff P(\alpha) = 0$ i.e $\pi_{m_\alpha} = \pi_\alpha$.
Ensuite, $\forall x \in \mathbb{Q}(\alpha),\ \chi_{m_\alpha}(x) = \det(x \operatorname{Id}_{\mathbb{Q}(\alpha)} - m_\alpha) = \det(y \mapsto (x - \alpha)y)$.
Donc $\chi_{m_\alpha}(\alpha) = \det(y \mapsto 0) = 0$ d'où $\pi_\alpha | \chi_{m_\alpha}$.
Ecrivons $\chi_{m_\alpha} = \pi_\alpha^r B$ avec $\pi_\alpha \wedge B = 1$ et $B \in \mathbb{Q}[X]$ ce qui est possible car π_α est irréductible dans $\mathbb{Q}[X]$ (cf. VI.32). D'après le théorème de Bézout il existe $U, V \in \mathbb{Q}[X]$ tels que $U\pi_\alpha + BV = 1$. En particulier cette relation montre que π_α et B n'ont pas de racines communes dans $\mathbb{C}$. si B est non constant alors il possède une racine $z \in \mathbb{C}$. Alors z est racine de χ_{m_α} pourtant les racines de χ_{m_α} sont les racines de $\pi_\alpha = \pi_{m_\alpha}$. Par conséquent B est constant et donc comme χ_{m_α} et π_α sont unitaires, $\chi_{m_\alpha} = \pi_\alpha^r$.

4. D'après la question 2, $\pi_{\sqrt{p_i p_j}} = X^2 - p_i p_j$. Et d'après la question 3, $\chi_{m_{\sqrt{p_i p_j}}} = (X^2 - p_i p_j)^r$ pour un certain $r \in \mathbb{N}^*$. Ce polynôme est pair de degré $2r$, le coefficient en X^{2r-1} est donc nul. Ainsi $\operatorname{Tr}(m_{\sqrt{p_i p_j}}) = 0$.
Ensuite, $\pi_{p_i} = X - p_i$. Donc $\chi_{m_{p_i}} = (X - p_i)^{r_i} = \sum_{k=0}^{r_i} \binom{r_i}{k} (-p_i)^{r_i - k} X^k$ pour un certain $r_i \in \mathbb{N}^*$. On en déduit que $\operatorname{Tr}(m_{p_i}) = -r_i p_i \neq 0$.
En outre $(\operatorname{Tr}(m_{\sqrt{p_i p_j}}))_{1 \leq i,j \leq n} = \operatorname{diag}(-r_k p_k,\ k \in [\![1; n]\!])$ est inversible.

5. On pose $\Phi : \left\{ \begin{array}{ccc} \mathbb{Q} & \longrightarrow & \mathbb{Q}^n \\ y & \longmapsto & (\operatorname{Tr}(m_{y\sqrt{p}_1}), \ldots, \operatorname{Tr}(m_{y\sqrt{p}_n})) \end{array} \right.$
Φ est $\mathbb{Q}$-linéaire comme composée d'applications linéaires. Si la famille $(\sqrt{p}_1, \ldots, \sqrt{p}_n)$ était $\mathbb{Q}$-liée alors la famille $(\Phi(\sqrt{p}_1), \ldots, \Phi(\sqrt{p}_n))$ le serait aussi. Ceci n'est pas possible puisque la matrice dont cette famille représente les lignes est inversible. Donc par contraposée, la famille $(\sqrt{p}_1, \ldots, , \sqrt{p}_n)$ est $\mathbb{Q}$-libre.

XIII.6.34 Corps des nombres algébriques ★★★★

[Enoncé]

Fixons $(x,y) \in \mathbb{A}^2$ avec $x \neq 0$. On note $P, Q \in \mathbb{Q}[X]$ tels que $P(x) = Q(y) = 0$. Quitte à les diviser par leurs coefficients dominants on peut supposer que P et Q sont unitaires.

Enfin on écrit $P(X) = \sum_{k=0}^{n} a_k X^k = \prod_{k=1}^{n}(X - \alpha_k)$ et $Q(X) = \sum_{k=0}^{m} b_k X^k = \prod_{k=1}^{m}(X - \beta_k)$.

— $\mathbb{A} \subset \mathbb{C}$. 0 est racine du polynôme X et 1 est racine du polynôme $X - 1$ donc $0, 1 \in \mathbb{A}$.

— $S(X) := P(-X) = \sum_{k=0}^{n}(-1)^k a_k X^k \in \mathbb{Q}[X]$ et $S(-x) = P(x) = 0$. Donc $-x \in \mathbb{A}$.

— $R(X) := X^n P\left(\frac{1}{X}\right) = \sum_{k=0}^{n} a_k X^{n-k} = \sum_{k=0}^{n} a_{n-k} X^k \in \mathbb{Q}[X]$ et $R\left(\frac{1}{x}\right) = \frac{P(x)}{x^n} = 0$. Donc $\frac{1}{x} \in \mathbb{A}$.

— On va construire A par blocs. Fixons $i \in [\![0; n-1]\!]$ et Notons $V_i = \begin{pmatrix} y^i \\ y^i x \\ \vdots \\ y^i x^{n-1} \end{pmatrix} = y^i V_0$.

On sait que la matrice compagnon de P : $C_P = \begin{pmatrix} 0 & \dots & \dots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \dots & 0 & 1 & -a_{n-1} \end{pmatrix}$ est à coefficients rationnels et admet x comme valeur propre. On remarque que $y^i V_0$ vecteur propre associé.

La matrice C_P ne dépend pas de i on va donc construire A comme étant la matrice diagonale par blocs

$$A = \left(\begin{array}{c|c|c|c} C_P & 0 & \cdots & 0 \\ \hline 0 & \ddots & \ddots & \vdots \\ \hline \vdots & \ddots & \ddots & 0 \\ \hline 0 & \cdots & 0 & C_P \end{array}\right)$$

On calcule

$$AV = A\left(\begin{array}{c} V_0 \\ \hline V_1 \\ \hline \vdots \\ \hline V_{n-1} \end{array}\right) = \left(\begin{array}{c} C_P V_0 \\ \hline C_P V_1 \\ \hline \vdots \\ \hline C_P V_{n-1} \end{array}\right) = \left(\begin{array}{c} xV_0 \\ \hline xV_1 \\ \hline \vdots \\ \hline xV_{n-1} \end{array}\right) = xV$$

Donc x est racine de χ_A. Or $\chi_A \in \mathbb{Q}[X]$ car ses coefficients sont polynomiaux en ceux de A qui sont rationnels et car $\mathbb{Q}$ est un anneau.
Pour B on va se ramener au cas précédent. On remarque qu'en permutant les coordonnées de V on peut se ramener à $W = \begin{pmatrix} 1 \\ y \\ y^2 \\ \vdots \\ y^{m-1} \\ x \\ yx \\ y^2x \\ \vdots \\ y^{m-1}x \\ \vdots \\ \vdots \\ y^{m-1}x^{n-1} \end{pmatrix}$. Formellement on pose la matrice de permutation $P = (\delta_{i,\sigma(j)})_{0\leq i,j\leq nm-1}$ avec σ la permutation de $[\![0; nm-1]\!]$ définie par $\forall k \in [\![0; nm-1]\!],\ \sigma(k) = j + im$ avec $k = i + jn$ la division euclidienne de k par n. P est construite de sorte à vérifier $W = PV$.
On a alors $B'W = yB$ avec $B' = \left(\begin{array}{c|c|c|c} C_Q & 0 & \cdots & 0 \\ \hline 0 & \ddots & \ddots & \vdots \\ \hline \vdots & \ddots & \ddots & 0 \\ \hline 0 & \cdots & 0 & C_Q \end{array}\right)$. D'où en posant $B = P^{-1}B'P$:
$BV = P^{-1}B'PV = P^{-1}B'W = P^{-1}(yW) = yP^{-1}(PV) = yV$.
B est bien à coefficients rationnels car, B' l'est et P l'est ce qui impose que son inverse aussi (cela découle de la formule $P^{-1} = \dfrac{1}{\det P}\operatorname{Com}(P)^\top$ en utilisant la structure de corps de $\mathbb{Q}$).
Finalement il reste à remarquer que $A + B, AB \in \mathcal{M}_{nm}(\mathbb{Q})$ et $(A + B)V = (x + y)V$ et $ABV = xyV$. $x + y$ est racine de $\chi_{A+B} \in \mathbb{Q}[X]$ et xy est racine de $\chi_{AB} \in \mathbb{Q}[X]$.

On conclut que $\mathbb{A}$ est un sous-corps de $\mathbb{C}$.

Remarque : Par la même démonstration on obtient que l'ensemble des entiers algébriques i.e l'ensemble des nombres complexes racines d'un polynôme unitaire à coefficients entiers non nul, est un sous-anneau de $\mathbb{C}$. Ce n'est cependant pas un corps car par exemple $\frac{1}{2}$ n'est pas un entier algébrique

XIII.6.35 Théorème de Kronecker ★★★★

[Enoncé]

1. On montre classiquement (cf. II.17) que pour tout polynôme unitaire $Q = X^n + \sum_{k=0}^{n-1} a_k X^k$ on a $Q = \chi_{C_Q}$ avec

$$C_Q = \begin{pmatrix} 0 & \dots & \dots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \dots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

   C_P est trigonalisable dans $\mathcal{M}_n(\mathbb{C})$ donc $\mathrm{Sp}(C_P^k) = \{\lambda^k,\ \lambda \in \mathrm{Sp}(C_p)\} = \{\lambda_1^k, \dots, \lambda_d^k\}$. $\lambda_1^k, \dots, \lambda_d^k$ sont donc les racines de $Q_k = \chi_{C_P^k}$ qui est unitaire.
   De plus, C_P est à coefficients entiers donc C_P^k est aussi à coefficients entiers. Par conséquent son polynôme caractéristique est aussi à coefficients entiers puisque ses coefficients sont polynomiaux en ceux de C_P^k et puisque $\mathbb{Z}$ est un anneau.

2. Notons $q_0, \dots, q_d$ les coefficients de Q_k. Par les relations coefficients racines on a :

$$\forall n \in [\![0; d]\!],\ q_{d-n} = (-1)^n \sum_{\substack{I \subset [\![1;d]\!] \\ \mathrm{Card}(I)=n}} \prod_{i \in I} \lambda_i^k$$

   Donc par inégalité triangulaire $\forall n \in [\![0; d]\!],\ |q_{d-n}| \leq \sum_{\substack{I \subset [\![1;d]\!] \\ \mathrm{Card}(I)=n}} \prod_{i \in I} |\lambda_i|^k = \sum_{\substack{I \subset [\![1;d]\!] \\ \mathrm{Card}(I)=n}} 1 = \binom{d}{n} \leq d!$.

3. Les coefficients de Q_k étant des entiers bornées, il ne peuvent prendre qu'un nombre fini de valeurs. D'après le principe des tiroirs, il existe une infinité d'entiers naturels non nuls $k \neq k'$ pour lesquels $Q_k = Q_{k'}$. De plus, les racines de Q_k étant en nombre fini quel que soit $k \in \mathbb{N}^*$ on en déduit finalement l'existence, quel que soit $i \in [\![0; d]\!]$, de deux entiers naturel non nuls $k_i \neq k_i'$ pour lesquels $\lambda_i^{k_i} = \lambda_i^{k_i'}$.
   Enfin comme $\lambda_i \neq 0$, cela implique $\lambda_i \in \mathbb{U}_{|k_i - k_i'|}$.

XIII.6.36 Irrationalité de e (1)

[Enoncé]

XIII.6.37 Irrationalité de e (2)

[Enoncé]

XIII.6.38 Irrationalité de π

[Enoncé]

XIII.6.39 Critère de transcendance de Liouville ★★★★

[Enoncé]

1. On sait qu'il existe $P \in \mathbb{Q}[X]$ non nul annulant α. Quitte à multiplier P par le ppcm des dénominateurs de ses coefficients, on peut supposer $P \in \mathbb{Z}[X]$. Notons $P = \sum_{k=0}^{d} a_k X^k$ où $d = \deg(P)$. P n'est pas nul et il s'annule donc il ne peut pas être constant, ainsi $d \geq 1$.
Fixons $n \in \mathbb{N}$.
$P\left(\frac{p_n}{q_n}\right) = \sum_{k=0}^{d} a_k \cdot \frac{p_n^k}{q_n^k} = \frac{1}{q_n^d} \sum_{k=0}^{d} a_k p_n^k q_n^{n-k}$.
Ainsi $q_n^d P\left(\frac{p_n}{q_n}\right) = \sum_{k=0}^{d} a_k p_n^k q_n^{n-k} \in \mathbb{Z}$.
De plus, si l'on considère $\varepsilon = \min\{|\alpha - z| \mid P(z) = 0, z \neq \alpha\}$ qui est strictement positif, comme $\frac{p_n}{q_n} \underset{n\to+\infty}{\longrightarrow} \alpha$ on sait que $\exists N \in \mathbb{N},\ \forall n \geq N,\ \left|\alpha - \frac{p_n}{q_n}\right| < \varepsilon$.
Ainsi $\forall n \geq N,\ P\left(\frac{p_n}{q_n}\right) \neq 0$. Et donc si $n \geq N$, $q_n^d P\left(\frac{p_n}{q_n}\right)$ est un entier non nul, on peut donc affirmer que $\left|q_n^d P\left(\frac{p_n}{q_n}\right)\right| \geq 1$ i.e $\frac{1}{q_n^d} \leq \left|P\left(\frac{p_n}{q_n}\right)\right|$.
Ensuite, fixons $n \geq N$. La fonction polynomiale associée à P est $\mathcal{C}^1$ sur le segment $[\alpha - \varepsilon, \alpha + \varepsilon]$ auquel α et $\frac{p_n}{q_n}$ appartiennent, donc d'après l'inégalité de Taylor-Lagrange :
$\left|P\left(\frac{p_n}{q_n}\right)\right| = \left|P\left(\frac{p_n}{q_n}\right) - P(\alpha)\right| \leq M \left|\alpha - \frac{p_n}{q_n}\right|$ avec $M = \sup_{x \in [\alpha-\varepsilon, \alpha+\varepsilon]} |P'(x)|$.
Finalement, $\forall n \geq N,\ \frac{1}{q_n^d} \leq M \left|\alpha - \frac{p_n}{q_n}\right|$ d'où $\frac{1}{q_n^d} \underset{n\to+\infty}{=} \mathcal{O}\left(\alpha - \frac{p_n}{q_n}\right)$.

Remarque : ce critère traduit le fait que les nombres algébriques sont en quelque sorte "mal approximable" par les rationnels ; dans le sens où, pour approximer un nombre algébrique α par des rationnels $\frac{p_n}{q_n}$, on va être obligé de prendre de grands dénominateurs

pour nos rationnels de sorte qu'ils soient de l'ordre de la racine d-ième de $\left|\alpha - \frac{p_n}{q_n}\right|$.

2. Comme la série en question converge très rapidement on va l'approcher par ses sommes partielles. Posons pour $n \in \mathbb{N}^*,\ S_n = \sum_{k=1}^{n} \frac{1}{10^{k!}}$.

   $(S_n)_{n\in\mathbb{N}^*}$ est une suite de rationnels qui converge vers $S = \sum_{n=1}^{+\infty} \frac{1}{10^{n!}}$.

   $\forall n \in \mathbb{N}^*,\ S_n = \dfrac{\sum_{k=1}^{n} 10^{n!-k!}}{10^{n!}}$.

   On cherche à montrer qu'il n'existe pas d'entier naturel non nul d et de constante $C \in \mathbb{R}_+^*$ tels que APCR,

   $\frac{1}{10^{dn!}} \leq C|S - S_n| = C \sum_{k=n+1}^{+\infty} \frac{1}{10^{k!}}$. Supposons par l'absurde que c'est le cas.

   Fixons $d \in \mathbb{N}^*$ et $C \in \mathbb{R}_+^*$. Fixons $n \in \mathbb{N}^*$. Si a et b sont deux entiers supérieurs ou égaux à 2 alors $ab \geq a + b$ (il suffit d'écrire, en supposant sans perte de généralité que $a \leq b$, que $a - 1 \geq 1 \geq a/b$) donc,

   $$\sum_{k=n+1}^{+\infty} \frac{1}{10^{k!}} \leq \frac{1}{10^{(n+1)!}} \sum_{k=n+1}^{+\infty} \frac{1}{10^{k(k-1)\ldots(n+2)}} \leq \frac{1}{10^{(n+1)!}} \sum_{k=n+1}^{+\infty} \frac{1}{10^{2^{k-n}}} \leq \frac{1}{10^{(n+1)!}} \sum_{k=1}^{+\infty} \frac{1}{10^k} =$$

   $$\frac{1}{10^{(n+1)!}} \cdot \frac{\frac{1}{10}}{1 - \frac{1}{10}} = \frac{1}{9 \times 10^{(n+1)!}}.$$

   Donc $\exists N \in \mathbb{N}^*,\ \forall n \geq N,\ 1 \leq \dfrac{C}{9} \cdot 10^{dn!-(n+1)!}$

   Or pour tout $n \geq d,\ (n+1)! = (n+1)n! > dn!$. Ainsi $\dfrac{C}{9} \cdot 10^{dn!-(n+1)!} \underset{n\to+\infty}{\longrightarrow} 0$.

   On obtient une absurdité donc S ne vérifie pas le critère d'où $\sum_{n=1}^{+\infty} \frac{1}{10^{n!}}$ est un nombre transcendant.

XIII.7 Correction Arithmétique

XIII.7.1 Infinité des nombres premiers ★★

[Enoncé]

1. Supposons par l'absurde qu'il existe un nombre fini de nombres premiers. On note alors $\mathbb{P} = \{p_1, \dots, p_n\}$ l'ensemble des nombres premiers et on pose $N = 1 + \prod_{k=1}^{n} p_k$.
   $\forall k \in [\![1; n]\!],\ N \equiv 1 \not\equiv 0[p_k]$. Donc N est un nombre premier qui n'appartient pas à $\mathbb{P}$ ce qui est absurde.
   On en déduit qu'il existe une infinité de nombres premiers.
2. Supposons par l'absurde qu'il existe un nombre fini de nombres premiers congrus à 3 modulo 4. On note alors $\mathbb{P}_4^3 = \{p_1, \dots, p_n\}$ l'ensemble des nombres premiers congrus à 3 modulo 4 et on pose $N = 2 + \prod_{k=1}^{n} p_k$ et $M = 4 + \prod_{k=1}^{n} p_k$.
   Pour tout $k \in [\![1; n]\!]$, $N \equiv 2[p_k]$ et $M \equiv 4[p_k]$. Or $2 \notin \mathbb{P}_4^3$ donc $2 \not\equiv 0[p_k]$ et $4 \not\equiv 0[p_k]$. Donc N et M sont des nombres premiers. De plus, si $n = 2r$ est pair alors $N \equiv 2 + \prod_{k=1}^{n} 3 \equiv 2 + 9^r \equiv 2 + 1^r \equiv 3[4]$, et si $n = 2r + 1$ est impair alors $M \equiv 4 + 3 \times 9^r \equiv 3[4]$. Dans tous les cas on peut construire un nouvel élément de $\mathbb{P}_4^3$ ce qui est absurde.
   On en déduit qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.

XIII.7.2 Version faible du théorème de progression arithmétique de Dirichlet

[Enoncé]

XIII.7.3 Racine carré d'un nombre premier ★★

[Enoncé]

Supposons par l'absurde que $\sqrt{p} \in \mathbb{Q}$. Alors il existe un couple d'entiers $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ premiers entre eux tel que $\sqrt{p} = \dfrac{a}{b}$.

Il suit que $pb^2 = a^2$. Intéressons nous à la valuation p-adique de a^2.

D'une part, si on écrit $a = \prod_{q \text{ premier}} q^{v_q(a)}$ la décomposition en facteur premier de a alors $a^2 = \prod_{q \text{ premier}} q^{2v_q(a)}$ d'où $v_p(a^2) = 2v_p(a)$ est paire.

D'autre part, par le même raisonnement la valuation p-adique de b^2 est paire mais alors

$v_p(a^2) = v_p(pb^2) = 1 + v_p(b^2)$ est impaire.
Ceci est absurde donc $\sqrt{p}$ n'est pas rationnel.

XIII.7.4 Une suite périodique

[Enoncé]

XIII.7.5 Racines de l'unité

[Enoncé]

XIII.7.6 Plus petit nombre premier ne divisant pas un entier donné

[Enoncé]

XIII.7.7 Théorème de Kurshak

[Enoncé]

XIII.7.8 Valuation p-adique de $\binom{p^n}{k}$

[Enoncé]

XIII.7.9 Une équation dans $\mathbb{N}$

[Enoncé]

XIII.7.10 Triplets pythagoriciens

[Enoncé]

XIII.7.11 Théorème de Sophie Germain ★★★

[Enoncé]

1. $x^p+y^p+z^p=0$ Donc en divisant par $(x\wedge y\wedge z)^p$ on obtient $\left(\frac{x}{x\wedge y\wedge z}\right)^p+\left(\frac{y}{x\wedge y\wedge z}\right)^p+\left(\frac{z}{x\wedge y\wedge z}\right)^p=0$ avec $\frac{x}{x\wedge y\wedge z}, \frac{y}{x\wedge y\wedge z}$ et $\frac{z}{x\wedge y\wedge z}$ des entiers premiers entre eux dans leur ensemble.
   On peut donc supposer, quitte à diviser par leur pgcd, que $x\wedge y\wedge z=1$. Soit k un diviseur premier commun à x et y. Alors $k|x^p+y^p=-z^p$. Or comme k est premier, d'après le lemme d'Euclide $k|z$ et donc $k|x\wedge y\wedge z=1$ ce qui est absurde car $k\geq 2$. On en déduit que x et y sont premiers entre eux. Par un raisonnement analogue, $x\wedge z=y\wedge z=1$.

2. a. Soit $(a,b,c)\in\mathbb{Z}^2$ tel que $ab=c^k$ et $a\wedge b=1$. Considérons un nombre premier r. On sait que la valuation r-adique de c^k est $v_r(c^k)=kv_r(c)$. D'autre part, $v_r(ab)=v_r(a)+v_r(b)$. Or comme $a\wedge b=1$, r divise au plus un et un seul des deux entiers a et b. Ainsi, on a toujours $v_r(ab)=v_r(a)$ ou $v_r(ab)=v_r(b)$. Par conséquent, $v_r(a)$ et $v_r(b)$ sont tous deux des multiples de k. On en déduit que a et b sont des puissances k-ième.

   b. On remarque que si $p=2$ alors $x^2+y^2+z^2=0\implies x=y=z=0$. Donc $p\neq 2$ et donc est impair. Ensuite, $y^p+z^p=-x^p\iff (x+y)\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k=(-x)^p$.
   Or si r est un diviseur premier commun à $y+z$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$ alors $y\equiv -z[r]$ et donc $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k\equiv\sum_{k=0}^{p-1}y^{p-1}\equiv py^{p-1}[r]$.
   Comme r est premier on en déduit que $r|p$ ou $r|y^{p-1}$ c'est à dire comme p est premier, $r=p$ ou, comme r est premier, $r|y$. Or si $r|y$ alors comme $r|y+z$, on obtient que $y|z=y+z-y$ ce qui est absurde car y et z sont premiers entre eux.
   Donc $r=p$ mais alors $-x^p=(y+z)\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k\equiv 0[p]$. Donc $p|-x^p$ puis $p|x$ et $xyz\equiv 0[p]$ ce qui est absurde.
   Ainsi $y+z$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$ n'ont pas de diviseurs premiers commun : ils sont donc premiers entre eux. La question précédente assure alors l'existence de deux entiers a et α tels que $y+z=a^p$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k=\alpha^p$.
   En réitérant le même raisonnement en isolant z puis y dans $x^p+y^p+z^p=0$ on obtient de même qu'il existe deux entiers b et c tels que $x+y=c^p$ et $x+z=b^p$.

3. Soit m un entier qui n'est pas un multiple de $q=2p+1$. D'après le petit théorème de Fermat $m^{q-1}=m^{2p}\equiv 1[q]$. Ceci se traduit dans $\mathbb{Z}/q\mathbb{Z}$:

$$\overline{m}^{2p}-\overline{1}=\overline{0}$$

ou encore :

$$\left(\overline{m}^p - \overline{1}\right)\left(m^p + \overline{1}\right) = \overline{0}$$

Or $\mathbb{Z}/q\mathbb{Z}$ est un corps car q est premier. Il est donc intègre d'où :

$$\overline{m}^p = \overline{1} \text{ ou } \overline{m}^p = \overline{-1}$$

Ainsi, $m^p \equiv \pm 1[q]$.
D'après ce qui vient d'être démontré, dans $\mathbb{Z}/q\mathbb{Z}$, $(\overline{x}^p, \overline{y}^p, \overline{z}^p) \in \{\overline{-1}, \overline{0}, \overline{1}\}^3$.
Si aucun des trois n'est nul alors $x^p + y^p + z^p \not\equiv 0[p]$ et donc $x^p + y^p + z^p \neq 0$ ce qui est absurde. Ainsi $x^p y^p z^p \equiv 0[q]$ c'est à dire $xyz \equiv 0[q]$.
Comme x, y, z sont deux à deux premiers entre eux, q ne divise qu'un seul d'entre eux.

4. $b^p + c^p - a^p = x + z + x + y - y - z = 2x \equiv 0[q]$.
$c^p = x + y \equiv y[q]$. De même, $z \equiv b^p[q]$.
D'après la question précédente, $y \equiv \pm 1[q]$ et $z \equiv \pm 1[q]$. Si $y \equiv z[q]$ alors $a^p \equiv \pm 2$ ce qui est absurde. Donc $y \equiv -z[q]$ c'est à dire $q|a^p$ puis $q|a$ car q est premier.
Enfin, $y \equiv -z[q] \implies \alpha^p \equiv \sum_{k=0}^{p-1} y^{p-1} = py^{p-1}[q]$.
On sait que $y \equiv c^p \equiv \pm 1[q]$. Donc comme $p-1$ est pair, $\alpha^p \equiv py^{p-1} \equiv p[q]$. De plus, $\alpha^p \equiv \pm 1[q]$ donc $p \equiv \pm 1[q]$.
C'est à dire qu'il existe un entier k tel que $p = kq \pm 1 = k(2p+1) \pm 1$.
Ceci est faux pour k négatif ou nul puis si $k \geq 1$, $p < kq \pm 1$.
On aboutit à une contradiction par conséquent il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0[p]$ et $x^p + y^p + z^p = 0$.

XIII.7.12 Une équation diophantienne

[Enoncé]

XIII.7.13 Calcul d'une somme

[Enoncé]

XIII.7.14 Nombres de Mersenne

[Enoncé]

XIII.7.15 Un exercice pour les années impaires

[Enoncé]

XIII.7.16 Equation du second degré dans $\mathbb{Z}/n\mathbb{Z}$

[Enoncé]

XIII.7.17 Un problème de congruence

[Enoncé]

XIII.7.18 Un multiple de 2026 qui ne s'écrit qu'avec des 2

[Enoncé]

XIII.7.19 Somme des puissances k-ièmes dans $\mathbb{Z}/p\mathbb{Z}$

[Enoncé]

XIII.7.20 Théorème de Wilson ★★

[Enoncé]
On travaille dans $\mathbb{Z}/p\mathbb{Z}$.
Si p n'est pas premier alors $\exists (m,n) \in [\![2;p-1]\!]^2,\ p = mn$. Par conséquent $(p-1)! = mn \times \prod_{k\in[\![1;p-1]\!]\setminus\{m,n\}} k = \overline{0} \neq \overline{-1}$.
Supposons que p est premier, autrement dit que $\mathbb{Z}/p\mathbb{Z}$ est un corps.
Alors par commutativité puis intégrité de $\mathbb{Z}/p\mathbb{Z}$, $\forall k \in \mathbb{Z}/p\mathbb{Z},\ k^2 = \overline{1} \iff (k-\overline{1})(k+\overline{1}) = 0 \iff k \in \{\overline{-1}, \overline{1}\}$.
Ceci montre que les seuls éléments de $\mathbb{Z}/p\mathbb{Z}$ qui sont égaux à leur inverse sont $\overline{-1}$ et $\overline{1} = \overline{p-1}$.
Par conséquent $(p-1)! = \prod_{k=1}^{p-1} \overline{k} = -\prod_{k=2}^{p-2} \overline{k} = -\overline{1}$ en rassemblant dans le produit, par commutativité, les facteurs deux à deux avec leur inverse.

XIII.7.21 Problème Putnam (2011) ★★★★★

[Enoncé]

Tout d'abord, comme p ne divise évidemment pas $\sum_{k=0}^{p-1} k!0^k = 1$ il suffit de montrer qu'il existe au moins $\frac{p+1}{2} - 1 = \frac{p-1}{2}$ valeurs de n dans $[\![1;p-1]\!]$ telles que p ne divise pas

$\sum_{k=0}^{p-1} k!n^k$.

Cela revient à montrer qu'il existe au plus $\frac{p-1}{2}$ valeurs de n dans $[\![1;p-1]\!]$ telles que p divise $\sum_{k=0}^{p-1} k!n^k$. Donnons nous alors $n \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $\sum_{k=0}^{p-1} k!n^k = \overline{0}$. On calcule :

$$\begin{aligned}
\sum_{k=0}^{p-1} k!n^k &= \sum_{k=0}^{p-1} (p-1-k)!n^{p-1-k} \\
&= \sum_{k=0}^{p-1} \overline{(p-1)!} \cdot \overline{(p-1)^{-1}} \dots \overline{(p-k+1)^{-1}} n^{p-1-k} \\
&= \sum_{k=0}^{p-1} -\overline{(p-1)^{-1}} \dots \overline{(p-k)^{-1}} n^{p-1-k} && \text{d'après le théorème de W} \\
&= \sum_{k=0}^{p-1} -\overline{(-1)^{-1}} \dots \overline{(-k)^{-1}} n^{-k} && \text{d'après le petit thé} \\
&= \sum_{k=0}^{p-1} \overline{k!}^{-1} (-n)^k && \text{Car } x \mapsto x^{-1} \text{ est un automorphisme de } (\\
&= \sum_{k=0}^{p-1} \overline{k!}^{-1} n^k && \text{Car } \overline{x} \mapsto \overline{p-x} = \overline{-x} \text{ est un automorph}
\end{aligned}$$

On pose le polynôme $P(X) = \sum_{k=0}^{p-1} \overline{k!}^{-1} X^k$ de $\mathbb{Z}/p\mathbb{Z}$. On cherche à montrer que $P(X)$ a au plus $\frac{p-1}{2}$ racines. D'après l'indication on sait déjà qu'il en a au plus $p-1$. Une idée peut alors être d'essayer de montrer que toutes ses racines sont doubles.

On va en fait montrer que les racines, dans $\mathbb{Z}/p\mathbb{Z}$, du polynôme $Q(X) = \sum_{k=0}^{p-1} \frac{X^k}{k!} - X + X^p$ de $\mathbb{R}[X]$ sont doubles.

P et Q coïncident sur $\mathbb{Z}/p\mathbb{Z}$ grâce au petit théorème de Fermat. De plus, 0 n'est pas racine de Q dans $\mathbb{Z}/p\mathbb{Z}$ et, si x n'est pas un multiple de p alors $Q'(x) = \sum_{k=1}^{p-1} \frac{x^{k-1}}{(k-1)!} - 1 + px^{p-1} \equiv \sum_{k=0}^{p-1} (k!)^{-1} x^k - ((p-1)!)^{-1} x^{p-1} - 1 \equiv \sum_{k=0}^{p-1} (k!)^{-1} x^k \equiv Q(x)[p]$.

Ainsi, si $\overline{n}$ est racine de P alors n est racine de Q et de Q' dans $\mathbb{Z}/p\mathbb{Z}$. Toutes les racines du polynôme Q dans $\mathbb{Z}/p\mathbb{Z}$ sont doubles donc celui-ci a au plus $\frac{p-1}{2}$ racines dans $\mathbb{Z}/p\mathbb{Z}$.

Ainsi P a au plus $\dfrac{p-1}{2}$ racines.

XIII.7.22 Critère d'Euler

[Enoncé]

XIII.7.23 Indicatrice d'Euler

[Enoncé]

1. Montrons que le seul sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ est $\mathbb{Z}/d\mathbb{Z}$.
   Il est clair que $\mathbb{Z}/d\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ car $d \mid n$.
   Soit H un sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$.
   Pour tout $x \in H, x^d = e$ d'après le théorème de Lagrange.
   Donc $H \subset \mathbb{Z}/d\mathbb{Z}$.
   Ainsi par égalité des cardinaux, $H = \mathbb{Z}/d\mathbb{Z}$. Maintenant, il suffit d'énumérer les éléments d'ordre exactement d qui les générateurs de $\mathbb{Z}/d\mathbb{Z}$.
   On en déduit donc qu'il y a $\varphi(d)$ éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$.
2. On partitionne $\mathbb{Z}/n\mathbb{Z}$ par les ensembles suivants :

   $$H_d = \{x \in \mathbb{Z}/n\mathbb{Z}, o(x) = d\} \text{ pour } d \mid n$$

   D'après la question précédente, $|H_d| = \varphi(d)$. Ces ensembles sont bien disjoints deux à deux et chaque élément de $\mathbb{Z}/n\mathbb{Z}$ appartient bien à un de ces ensembles d'après le théorème de Lagrange.
   Ainsi :

   $$\mathbb{Z}/n\mathbb{Z} = \bigsqcup_{d|n} H_d$$

   Donc par passage au cardinal :

   $$n = \sum_{d|n} \varphi(d)$$

3. On remarque ainsi que

   $$\varphi(n) = n - \sum_{d|n et d \neq n} \varphi(d)$$

```python
def ind_euler(n):
 L=[]
 s=0
  for i in range(1,n) :
   if n%i==0:
    L.append(i)
  for d in L:
```

```
8                    s+= ind_euler(d)
9                return n-s
```

XIII.7.24 Une minoration de l'indicatrice d'Euler

[Enoncé]

1. Sans perte de généralités, supposons que les n_i sont rangées dans l'ordre décroissant. Ainsi puisque les (n_i) sont des entiers ont en déduit les inégalités suivantes :

$$\forall i \in [\![2;k]\!], \quad n_i \geq n_1 + i - 1$$

Par conséquent :

$$\prod_{i=1}^{k}\left(1-\frac{1}{n_i}\right) \geq \prod_{i=1}^{k}\frac{n_1+i-2}{n_1+i-1} = \frac{n_1-1}{n_1+k-1}.$$

L'étude de la fonction : $x \mapsto \frac{x-1}{x+k-1}$ sur $[2,+\infty[$ donne :

$$\prod_{i=1}^{k}\left(1-\frac{1}{n_i}\right) \geq \frac{1}{k+1}.$$

2. Soit $n \in \mathbb{N}^*$.

On décompose n en facteurs premiers : $n = \prod_{i=1}^{k} p_i^{\alpha_i}$.

D'après le cours : $\varphi(n) = n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$.

Ainsi d'après la question précédente, $\varphi(n) \geq \frac{n}{k+1}$.

De plus, $n \geq \prod_{i=1}^{k} p_i \geq 2^k$ donc $2n \geq 2^{k+1}$ et donc $\ln(2n) \geq (k+1)\ln(2)$.

Par conséquent, $\varphi(n) \geq \frac{n\ln(2)}{\ln(2n)}$

XIII.7.25 Théorème d'interversion de Möbius

[Enoncé]

1. 1 est le produit de 0 nombre premiers distincts, donc : $\mu(1) = (-1)^0 = 1 \neq 0$. Soit $(m,n) \in (\mathbb{N}^*)^2$ tel que $m \wedge n = 1$. Si m ou n est divisible par le carré d'un nombre premier, alors mn l'est également. Donc :

$$\mu(mn) = 0 = \mu(m)\mu(n)$$

Sinon, si m et n n'est pas divisible par le carré d'un nombre premier, alors mn n'est pas divisible par le carré d'un nombre premier car m et n sont premiers entre eux i.e. m n n'ont pas de facteurs premiers communs.
En notant k (resp. l) le nombre de facteur premiers distincts intervenant dans la décomposition en facteurs premiers de m (resp. n), on en déduit que mn est le produit de $k+l$ nombres premiers. Ainsi :

$$\mu(mn) = (-1)^{k+l} = (-1)^k(-1)^l = \mu(m)\mu(n)$$

Donc μ est multiplicative.

2. Il s'agit de montrer que :

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \geq 2 \end{cases}$$

Soient $p_1, \dots, p_r$ les diviseurs premiers deux à deux distincts de l'entier n. Par définition de μ, les seuls diviseurs positifs qui de n qui vont intervenir dans la somme sont ceux de la forme :

$$p_I = p_{i_1} \dots p_{i_r}$$

où $I = \{i_1, \dots, i_r\}$ est une partie de $[\![1; r]\!]$. On a alors :

$$\sum_{d|n} \mu(d) = \sum_{I} (-1)^{|I|}$$

Or pour tout $s \in [\![0; r]\!]$, il y a $\binom{r}{s}$ parties I de $[\![1; r]\!]$ à s éléments.
Ainsi,

$$\sum_{d|n} \mu(d) = \sum_{s=0}^{r} \binom{r}{s} (-1)^s = (1-1)^r$$

Finalement, on en déduit bien que :

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \geq 2 \end{cases}$$

3. Soit $n \in \mathbb{N}^*$ Remarquons l'équivalence suivante :

$$\forall d, d' \geq 1,\ d|n \text{ et } d'|\frac{n}{d} \iff d'|n \text{ et } d|\frac{n}{d}$$

$$\begin{aligned}\sum_{d|n}\mu(d)F\Big(\frac{n}{d}\Big) &= \sum_{d|n}\mu(d)\sum_{d'|\frac{n}{d}}f(d')\\ &= \sum_{d|n}\sum_{d'|\frac{n}{d}}\mu(d)f(d')\\ &= \sum_{d'|n}\sum_{d|\frac{n}{d'}}\mu(d)f(d') \qquad \text{(d'après l'équivalence précédente)}\\ &= \sum_{d'|n}f(d')\sum_{d|\frac{n}{d'}}\mu(d)\end{aligned}$$

D'après la question 2,

$$\sum_{d|\frac{n}{d'}}\mu(d)\neq 0 \iff d'=n$$

Par conséquent, on en déduit bien l'égalité souhaité :

$$f(n)=\sum_{d|n}\mu(d)F(\frac{n}{d})$$

4. D'après l'exercice VII.23, on a :

$$I(n)=n=\sum_{d|n}\varphi(d)$$

Ainsi d'après la formule d'inversion de Möbius, on a :

$$\varphi(n)=\sum_{d|n}\mu(d)\frac{n}{d}$$

i.e

$$\varphi=\mu*I$$

XIII.7.26 Probabilité que deux entiers soient premiers entre eux

[Enoncé]

XIII.7.27 Limite d'une fonction arithmétique multiplicative

[Enoncé]

XIII.7.28 Fonctions arithmétiques réelles additives

[Enoncé]

XIII.7.29 Une majoration de la somme des diviseurs d'un entier

[Enoncé]

XIII.7.30 Entiers algébriques

[Enoncé]

XIII.7.31 Majoration de la primorielle

[Enoncé]

1. — Pour $n=1$ $\prod_{\substack{p\leq 1\\ p\text{premier}}} p = 1 \leq 4^1$.
   — Pour $n=2$, $\prod_{\substack{p\leq 2\\ p\text{premier}}} p = 2 \leq 4^2 = 16$.
   — Pour $n=3$, $\prod_{\substack{p\leq 3\\ p\text{premier}}} p = 6 \leq 4^3 = 64$.
2. Soit $n \geq 4$ un entier pair.
   Puisque n est pair, il ne peut être premier, ainsi :
   $$\prod_{\substack{p\leq n\\ p\text{premier}}} p = \prod_{\substack{p\leq n-1\\ p\text{premier}}} p$$
   Ainsi, d'après l'hypothèse de récurrence, le résultat est vrai.*
3. Soit p un nombre premier tel que $m+1 < p \leq 2m+1$. Alors p apparaît dans la décomposition en facteurs premiers de $(2m+1)!$ (au moins une fois), tandis que ni $m!$ ni $(m+1)!$ ne contiennent p (car tous leurs facteurs sont $\leq m+1 < p$). Par conséquent la puissance de p dans le numérateur est strictement supérieure à sa puissance dans le dénominateur, et donc p divise $\binom{2m+1}{m}$.
   Ainsi le produit des nombres premiers situés dans l'intervalle $m+1 < p \leq 2m+1$ divise $\binom{2m+1}{m}$. En particulier
   $$\prod_{\substack{p \text{ premier}\\ m+1<p\leq 2m+1}} p \;\Big|\; \binom{2m+1}{m} \quad\Longrightarrow\quad \prod_{\substack{p \text{ premier}\\ m+1<p\leq 2m+1}} p \leq \binom{2m+1}{m}.$$
   Les coefficients binomiaux de l'expansion de $(1+1)^{2m+1} = 2^{2m+1}$ satisfont, par symétrie,
   $$\binom{2m+1}{m} = \binom{2m+1}{m+1},$$

donc

$$2\binom{2m+1}{m} = \binom{2m+1}{m} + \binom{2m+1}{m+1} \leq \sum_{k=0}^{2m+1} \binom{2m+1}{k} = 2^{2m+1}.$$

D'où

$$\binom{2m+1}{m} \leq 2^{2m} = 4^m.$$

En combinant les deux observations on obtient

$$\prod_{\substack{p \text{ premier} \\ m+1<p\leq 2m+1}} p \leq \binom{2m+1}{m} \leq 4^m.$$

4. Par hypothèse de récurrence (valable pour tous les entiers strictement inférieurs à n), on a en particulier

$$\prod_{\substack{p \text{ premier} \\ p\leq m}} p \leq 4^m.$$

Donc le produit de tous les nombres premiers $\leq n = 2m+1$ se factorise en

$$\prod_{\substack{p \text{ premier} \\ p\leq 2m+1}} p = \left(\prod_{p\leq m} p\right) \cdot \left(\prod_{\substack{p \text{ premier} \\ m+1<p\leq 2m+1}} p\right) \leq 4^m \cdot 4^m = 4^{2m} = 4^{n-1}.$$

En particulier on obtient bien la majoration cherchée

$$\prod_{\substack{p \text{ premier} \\ p\leq n}} p \leq 4^n.$$

XIII.7.32 Théorèmes de Mertens

[Enoncé]

XIII.7.33 Théorèmes de Tchebychev

[Enoncé]

XIII.8 Correction Dénombrement

XIII.8.1 Identité de Vandermonde

[Enoncé]

Formule de Chu-Vandermonde

XIII.8.2 Nombre de Fibonacci

[Enoncé]

XIII.8.3 Matrices orthogonales à coefficients entiers

[Enoncé]

XIII.8.4 Nombre de carrés inférieur à un entier fixé ★

[Enoncé]
Fixons $n \in \mathbb{N}$.
$\forall k \in \mathbb{Z},\ k^2 \in A(n) \iff 0 < k^2 \leq n \iff 0 < |k| \leq \sqrt{n} \iff 0 < |k| \leq \lfloor \sqrt{n} \rfloor$.
Donc $\text{Card}(A(n)) = \lfloor \sqrt{n} \rfloor$.

XIII.8.5 Dérangement

[Enoncé]

XIII.8.6 Dérangement partiel

[Enoncé]

XIII.8.7 Nombres de Bell

[Enoncé]

XIII.8.8 Nombres de Catalan

[Enoncé]

XIII.8.9 Nombres de parties

[Enoncé]

XIII.8.10 Nombre de surjection

[Enoncé]

XIII.8.11 Formule de Legendre

[Enoncé]

XIII.8.12 Théorème de Hall ★★★★

[Enoncé]
(i) $\implies$ (ii) :
Supposons que l'on dispose de $x_1 \in A_1, \dots, x_n \in A_n$ tous distincts et donnons nous une partie I de $[\![1;n]\!]$.
$\{x_i,\ i \in I\} \subset \bigcup_{i\in I} A_i$ donc $\text{Card}\left(\bigcup_{i\in I} A_i\right) \geq \text{Card}(\{x_i,\ i \in I\}) = \text{Card}(I)$.
(ii) $\implies$ (i) :
Par récurrence forte sur $n \in \mathbb{N}^*$.
$n = 1$:
Si l'on dispose de $A_1 \subset E$ tel que $\text{Card}(A_1) \geq \text{Card}([\![1;1]\!]) = 1$ alors il existe $x_1 \in A_1$ et la preuve est terminée.
Supposons le résultat vrai, pour tout $k \in [\![1;n]\!]$, pour un certain $n \in \mathbb{N}^*$ et donnons nous $A_1, \dots, A_{n+1} \subset E$ pour lesquels on ai (ii).
Dans la suite on appellera *système de représentant* de la famille $(A_i)_{i\in I}$ toute famille $(x_i)_{i\in I} \in \prod_{i\in I} A_i$ dont les éléments sont tous distincts. Considérons $\mathcal{I} = \{I \in \mathcal{P}([\![1;n+1]\!])\backslash\{\emptyset, [\![1;n+1]\!]\},\ \text{Card}(A_I) = \text{Card}(I)\}$ où pour $I \subset [\![1;n+1]\!]$, A_I désigne la réunion $\bigcup_{i\in I} A_i$.
Dans un premier temps supposons que $\mathcal{I}$ est vide, autrement dit que $\forall I \subset [\![1;n+1]\!],\ 1 \leq \text{Card}(I) \leq n \implies \text{Card}(A_I) > \text{Card}(I)$.
Considérons $x_{n+1} \in A_{n+1}$ puis posons pour $i \in [\![1;n]\!]$, $B_i = A_i\backslash\{x_{n+1}\}$. Montrons que la famille $(B_i)_{1\leq i\leq n}$ satisfait (ii).
Soit $I \subset [\![1;n]\!]$ non vide.
$$\text{Card}\left(\bigcup_{i\in I} B_i\right) = \text{Card}\left(\bigcup_{i\in I} A_i\backslash\{x_{n+1}\}\right) = \text{Card}\left(\left(\bigcup_{i\in I} A_i\right)\backslash\{x_{n+1}\}\right) \geq \text{Card}\left(\bigcup_{i\in I} A_i\right) -$$

$1 > \text{Card}(I) - 1$.
Donc $\text{Card}\left(\bigcup_{i\in I} B_i\right) \geq \text{Card}(I)$.
On en déduit par hypothèse de récurrence qu'il existe un système de représentant $(x_i)_{1\leq i\leq n}$ de $(B_i)_{1\leq i\leq n}$. Mais alors par construction, $x_{n+1} \in A_{n+1}$ et pour tout $(i,j) \in [\![1;n]\!]^2$ distincts, $x_i \in A_i$ et $x_i \neq x_{n+1}$ et $x_i \neq x_j$. Donc $(x_i)_{1\leq i\leq n+1}$ est un système de représentant de $(A_i)_{1\leq i\leq n+1}$.

Supposons maintenant que $\mathcal{I}$ n'est pas vide et fixons $I \in \mathcal{I}$. $1 \leq \text{Card}(I) \leq n$ donc en appliquant l'hypothèse de récurrence à $(A_i)_{i\in I}$, qui vérifie bien (ii), il existe un système de représentant $(y_i)_{i\in I}$ de $(A_i)_{i\in I}$.
On pose alors $K = [\![1;n+1]\!]\backslash I$ puis pour tout $k \in K$, $C_k = A_k \backslash A_I$. Montrons $(C_k)_{k\in K}$ vérifie (ii).
Soit $J \subset K$.
$$\text{Card}\left(\bigcup_{j\in J} C_j\right) = \text{Card}\left(\bigcup_{j\in J} A_j\backslash A_I\right) = \text{Card}\left(\left(\bigcup_{j\in J} A_j\right)\backslash A_I\right) = \text{Card}\left(\left(\bigcup_{i\in J\cup I} A_j\right)\backslash A_I\right) \geq$$
$$\text{Card}\left(\bigcup_{j\in J\cup I} A_j\right) - \text{Card}(A_I).$$
Or $I \in \mathcal{I}$ donc $\text{Card}(A_I) = \text{Card}(I)$ et par (ii) $\text{Card}\left(\bigcup_{j\in J\cup I} A_j\right) \geq \text{Card}(J\cup I)$. De plus, l'union $J \cup I$ est disjointe puisque J est inclus dans le complémentaire de I.
On en déduit que $\text{Card}\left(\bigcup_{j\in J} C_j\right) \geq \text{Card}(J\cup I) - \text{Card}(I) = \text{Card}(J)$.
Enfin $1 \leq \text{Card}(K) \leq n$ donc par hypothèse de récurrence il existe un système de représentant $(y_i)_{i\in K}$ de $(C_k)_{k\in K}$.
Mais alors par construction si $k \in K$, $y_k \in A_k$ n'est pas un élément de la famille $(y_i)_{i\in I\cup K\backslash\{k\}}$.
Ainsi $(y_i)_{i\in I\cup K}$ est un système de représentant de $(A_i)_{1\leq i\leq n+1}$ ce qui termine l'hérédité.

XIII.8.13 Formule du Crible

[Enoncé]

XIII.8.14 Cardinal de $GL_n(K)$ et $SL_n(K)$

[Enoncé]

XIII.8.15 $\mathbb{Q}$ est dénombrable

[Enoncé]

XIII.8.16 $\mathbb{R}$ n'est pas dénombrable

[Enoncé]

XIII.8.17 Dénombrabilité des nombres algébriques

[Enoncé]

XIII.8.18 Théorème de Cantor

[Enoncé]

XIII.8.19 Fonction qui intervertit rationnels et irrationnels

[Enoncé]

XIII.8.20 Support d'une famille sommable

[Enoncé]

XIII.8.21 Théorème de Froda

[Enoncé]

XIII.8.22 Ensemble discret

[Enoncé]

XIII.8.23 Ensemble parfait

[Enoncé]

Poussière de Cantor

Ensemble parfait de $\mathbb{R}$

Théorème de Cantor-Berdixson

XIII.9 Correction Probabilités

XIII.9.1 Somme de variables de Bernoulli indépendantes ★★

[Enoncé]
Tout d'abord, $X(\Omega) = [\![0; n]\!]$. Notons, pour $k \in [\![0; n]\!]$, E_k l'ensemble des parties de $[\![1; n]\!]$ a k éléments. Fixons $k \in [\![0; n]\!]$.
Pour que $X = k$ il est nécessaire et suffisant de choisir k indices i dans $[\![1; n]\!]$ pour lesquels on ait $X_i = 1$ et $X_j = 0$ pour les $n - k$ autres indices j :

$$\{X = k\} = \bigsqcup_{I \in E_k} \left(\bigcap_{i \in I} \{X_i = 1\} \bigcap_{j \in [\![1;n]\!] \setminus I} \{X_j = 0\} \right)$$

Ainsi,

$$\begin{aligned}
\mathbb{P}(X = k) &= \sum_{I \in E_k} \mathbb{P}\left(\bigcap_{i \in I} \{X_i = 1\} \bigcap_{j \in [\![1;n]\!] \setminus I} \{X_j = 0\} \right) \\
\text{(par indépendance)} \quad &= \sum_{I \in E_k} \left(\prod_{i \in I} \mathbb{P}(X_i = 1) \prod_{j \in [\![1;n]\!] \setminus I} \mathbb{P}(X_j = 0) \right) \\
&= \sum_{I \in E_k} \left(\prod_{i \in I} p \prod_{j \in [\![1;n]\!] \setminus I} (1 - p) \right) \\
&= \sum_{I \in E_k} p^{\mathrm{Card}(I)} (1 - p)^{\mathrm{Card}([\![1;n]\!] \setminus I)} \\
&= \sum_{I \in E_k} p^k (1 - p)^{n-k} \\
&= \mathrm{Card}(E_k) p^k (1 - p)^{n-k} \\
&= \binom{n}{k} p^k (1 - p)^{n-k}
\end{aligned}$$

$X \sim \mathcal{B}(n, p)$.

XIII.9.2 Approximation de la loi de Poisson par des lois binomiales ★

[Enoncé]
Soit $k \in \mathbb{N}$.
$\forall n \in \mathbb{N},\ \mathbb{P}(X_n = k) = \binom{n}{k} p_n^k (1 - p_n)^{n-k} = \dfrac{n!}{k!(n-k)!} p_n^k (1 - p_n)^{n-k}$.

Donc d'après la formule de Stirling,

$$\begin{aligned}\mathbb{P}(X_n = k) &\underset{n\to+\infty}{\sim} \frac{p_n^k(1-p_n)^{n-k}}{k!} \cdot \frac{\left(\frac{n}{e}\right)^n \sqrt{2\pi n}}{\left(\frac{n-k}{e}\right)^{n-k} \sqrt{2\pi(n-k)}} \\ &\underset{n\to+\infty}{\sim} \frac{p_n^k(1-p_n)^{n-k}}{k!} \left(\frac{n}{n-k}\right)^n e^k (n-k)^k \\ &\underset{n\to+\infty}{\sim} \frac{(np_n)^k(1-p_n)^{n-k}}{k!} e^{n(\ln(n)-\ln(n-k))} e^k \\ &\underset{n\to+\infty}{\sim} \frac{\lambda^k e^{(n-k)\ln(1-p_n)}}{k!} e^{-n\ln(1-k/n)} e^k\end{aligned}$$

Or $np_n \underset{n\to+\infty}{=} \mathcal{O}(1)$ donc $p_n \underset{n\to+\infty}{\longrightarrow} 0$ d'où $(n-k)\ln(1-p_n) \underset{n\to+\infty}{\sim} (n-k)(-p_n) \underset{n\to+\infty}{\sim} -\lambda$ et puis $e^{(n-k)\ln(1-p_n)} \underset{n\to+\infty}{\sim} e^{-\lambda}$.

De plus, $-n\ln\left(1-\frac{k}{n}\right) \underset{n\to+\infty}{\longrightarrow} -k$ d'où $e^{-n\ln(1-k/n)} \underset{n\to+\infty}{\sim} e^{-k}$.

Ainsi, $\mathbb{P}(X_n = k) \underset{n\to+\infty}{\longrightarrow} \frac{\lambda^k e^{-\lambda}}{k!}$.

XIII.9.3 Inégalité de Markov et inégalité de Bienaymé-Tchébychev ★

[Enoncé]

Inégalité de Markov :
Si $X \in L^1$ est une variable aléatoire réelle positive et $a \in \mathbb{R}_+^*$ alors,

$$\mathbb{P}(X \geq a) \leq \frac{\mathbb{E}(X)}{a}$$

Soient $X \in L^1$ est une variable aléatoire réelle positive et $a \in \mathbb{R}_+^*$.

$$\mathbb{P}(X \geq a) = \sum_{\substack{x\in X(\Omega)\\ x\geq a}} \mathbb{P}(X = x) \leq \sum_{\substack{x\in X(\Omega)\\ x\geq a}} \frac{x}{a}\mathbb{P}(X = x) \leq \frac{1}{a}\sum_{x\in X(\Omega)} x\mathbb{P}(X = x) = \frac{\mathbb{E}(X)}{a}.$$

Inégalité de Bienaymé-Tchébychev :
Si $X \in L^2$ et $\varepsilon \in \mathbb{R}_+^*$ alors,

$$\mathbb{P}(|X - \mathbb{E}(X)| \geq \varepsilon) \leq \frac{\mathbb{V}(X)}{\varepsilon^2}$$

Soient $X \in L^2$ et $\varepsilon \in \mathbb{R}_+^*$.
$Y = (X - \mathbb{E}(X))^2$ est une variable aléatoire réelle positive d'espérance finie, en effet son espérance est $\mathbb{V}(X) < +\infty$.

D'après l'inégalité de Markov,

$$\mathbb{P}(|X - \mathbb{E}(X)| \geq \varepsilon) = \mathbb{P}(Y \geq \varepsilon^2) \leq \frac{\mathbb{E}(Y)}{\varepsilon^2} = \frac{\mathbb{V}(X)}{\varepsilon^2}$$

XIII.9.4 Paradoxe des anniversaires ★★

[Enoncé]
Notons A_n l'évènement "Aucun des n élèves de la classe ne sont nés le même jour" de sorte que $\mathbb{P}(A_n) = 1 - p_n$.
Notons pour $k \in [\![1; n]\!]$, X_k la variable aléatoire qui associe au k-ième élève associe son jour de naissance ($X_k(\Omega) = [\![1; 365]\!]$).
L'énoncé nous invite à munir Ω de la probabilité uniforme pour laquelle on a $\forall (k, j) \in [\![1; n]\!] \times [\![1; 365]\!]$, $\mathbb{P}(X_k = j) = \dfrac{1}{365}$.
Alors $A_n = \bigcap_{k=1}^{n} \left(\bigcap_{p=1}^{k-1} \{X_k \neq X_p\} \right)$ et en supposant l'indépendance des X_k (ce qui revient à ne pas prendre en compte les situations du type jumeaux par exemple) :

$$\begin{aligned}
p_n &= 1 - \prod_{k=1}^{n} \prod_{p=1}^{k-1} \mathbb{P}(X_k \neq X_p) \\
&= 1 - \prod_{k=1}^{n} \prod_{p=1}^{k-1} \sum_{j=1}^{365} \mathbb{P}(X_k = j, X_p \neq j) \\
\text{(par indépendance)} &= 1 - \prod_{k=1}^{n} \prod_{p=1}^{k-1} \sum_{j=1}^{365} \mathbb{P}(X_k = j)\mathbb{P}(X_p \neq j) \\
&= 1 - \prod_{k=1}^{n} \prod_{p=1}^{k-1} \sum_{j=1}^{365} \frac{1}{365} \cdot \frac{364}{365} \\
&= 1 - \prod_{k=1}^{n} \prod_{p=1}^{k-1} \frac{364}{365} \\
&= 1 - \prod_{k=1}^{n} \left(\frac{364}{365} \right)^{k-1} \\
&= 1 - \left(\frac{364}{365} \right)^{\sum_{k=1}^{n} (k-1)} \\
&= 1 - \left(\frac{364}{365} \right)^{\frac{n(n-1)}{2}}
\end{aligned}$$

Ainsi, $p_n > 0,5 \iff \left(\frac{364}{365}\right)^{\frac{n(n-1)}{2}} < 0,5 \iff \frac{n(n-1)}{2}\ln\left(\frac{364}{365}\right) < \ln(0,5) \iff n(n-1) > \frac{2\ln(2)}{\ln\left(\frac{365}{364}\right)} \approx 505,3.$

On calcule $23 \times 22 = 506$ donc à partir de $n = 23$ élèves, il y a plus d'une chance sur 2 pour que deux élèves aient la même date d'anniversaire.
Pour $n = 50$, $p_n \approx 0,965$.

XIII.9.5 Variable aléatoire presque sûrement nulle/constante

[Enoncé]

1. D'après la formule de transfert, on a :

$$\mathbb{E}(|X|) = \sum_{x \in X(\Omega)} |x|\mathbb{P}(X = x)$$

Il s'agit d'une somme à termes positifs, ainsi on en déduit que

$$\forall x \in X(\Omega), |x|\mathbb{P}(X = x) = 0$$

Par conséquent,

$$\forall x \in X(\Omega), |x| = 0 \text{ ou } \mathbb{P}(X = x) = 0$$

Donc pour tout $x \in X(\Omega)$ non nul, on a $\mathbb{P}(X = x) = 0$. Par conséquent,

$$\mathbb{P}(X = 0) = 1$$

2. On sait que $\mathbb{V}(X) = \mathbb{E}(|X - \mathbb{E}(x)|)$, donc en posant $Y = X - \mathbb{E}(X)$, d'après la question 1, on a que

$$Y \text{ est presque surement nulle}$$

Donc

$$\mathbb{P}(X - \mathbb{E}(X) = 0) = 1$$

Donc en posant $a = \mathbb{E}(X)$, on a le résultat.

XIII.9.6 Loi de Pascal ★★

[Enoncé]

1. La variable aléatoire T_r peut être interprétée comme celle qui indique le premier rang d'obtention du r-ième succès d'une expérience de Bernoulli que l'on répète indéfiniment. Pour $r = 1$ on reconnaît l'interprétation d'une loi géométrique. C'est donc ce que l'on va montrer.

Il est clair que $T_1(\Omega) = \mathbb{N}^* \cup \{+\infty\}$. Fixons $k \in \mathbb{N}^*$.
$\{T_1 = k\} = \{X_k = 1\} \cap \bigcap_{i=1}^{k-1} \{X_i = 0\}$.

Donc par indépendance, $\mathbb{P}(T_1 = k) = \mathbb{P}(X_k = 1) \prod_{i=1}^{k-1} \mathbb{P}(X_i = 0) = p(1-p)^{k-1}$.

Ainsi, $T_1 \sim \mathcal{G}(p)$.

2. Soit $n \in \mathbb{N}^*$.
D'après le cours, $S_n = \sum_{k=1}^{n} X_k \sim \mathcal{B}(n,p)$ donc $\mathbb{P}(S_n = r-1) = \binom{n}{r-1} p^{r-1}(1-p)^{n-r+1}$.
Ensuite, $\{T_r = n\} = \{S_n = r\} \cap \{S_{n-1} = r-1\}$.
Donc $\mathbb{P}(T_r = n) = \mathbb{P}(S_{n-1} = r-1)\mathbb{P}(S_n = r \mid S_{n-1} = r-1) = \mathbb{P}(S_{n-1} = r-1)\mathbb{P}(X_n = 1) = \binom{n-1}{r-1} p^r (1-p)^{n-r}$.
On remarque d'ailleurs que cette expression reste valide pour $r < n$.

3. $\overline{\{T_r = +\infty\}} = \bigsqcup_{n \in \mathbb{N}^*} \{T_r = n\}$ donc

$$\begin{aligned}
\mathbb{P}(\overline{T_r = +\infty}) &= \sum_{n=1}^{+\infty} \mathbb{P}(T_r = n) \\
&= \sum_{n=1}^{+\infty} \binom{n-1}{r-1} p^r (1-p)^{n-r} \\
&= \sum_{n=r}^{+\infty} \binom{n-1}{r-1} p^r (1-p)^{n-r} \\
&= \frac{p^r}{(r-1)!} \sum_{n=r}^{+\infty} \frac{(n-1)!}{(n-r)!} (1-p)^{n-r} \\
&= \frac{p^r}{(r-1)!} \sum_{n=r-1}^{+\infty} \frac{n!}{(n+1-r)!} (1-p)^{n+1-r}
\end{aligned}$$

On reconnaît la somme de la dérivée $r-1$-ième de la série géométrique en $1-p \in]-1,1[$:
$\sum_{n=r-1}^{+\infty} \frac{n!}{(n+1-r)!} x^{n+1-r} = \frac{d^{r-1}}{dx^{r-1}} \left(\sum_{n=0}^{+\infty} x^n \right) = \frac{d^{r-1}}{dx^{r-1}} \left(\frac{1}{1-x} \right) = \frac{(r-1)!}{(1-x)^r}$.
D'où $\mathbb{P}(\overline{T_r = +\infty}) = \frac{p^r}{(r-1)!} \cdot \frac{(r-1)!}{p^r} = 1$ et $\mathbb{P}(T_r = +\infty) = 0$.

XIII.9.7 Lemme de Borel-Cantelli et loi du zéro-un de Borel ★★★

[Enoncé]

1. a. $\forall n \in \mathbb{N},\ B_{n+1} \subset B_n$ donc par continuité décroissante, $\mathbb{P}(A) = \mathbb{P}\left(\bigcap_{n\in\mathbb{N}} B_n\right) = \lim_{n\to+\infty} \mathbb{P}(B_n)$.

   b. $\forall n \in \mathbb{N},\ \mathbb{P}(B_n) \leq \sum_{k=n}^{+\infty} \mathbb{P}(A_k)$. Or comme la série $\sum_{n\in\mathbb{N}} \mathbb{P}(A_n)$ converge, on sait que $\lim_{n\to+\infty} \sum_{k=n}^{+\infty} \mathbb{P}(A_k) = 0$ d'où $\mathbb{P}(A) = 0$.

2. Rappelons que ln est concave sur $\mathbb{R}_+^*$ et donc que $\forall x \in \mathbb{R}_+^*,\ \ln(x) \leq \ln'(1)(x-1) + \ln(1) = x - 1$. De plus, par indépendance, $\mathbb{P}\left(\bigcap_{k=n}^{n+p} \overline{A_k}\right) = \prod_{k=n}^{n+p} \mathbb{P}(\overline{A_k})$.
   Si $\mathbb{P}\left(\bigcap_{k=n}^{n+p} \overline{A_k}\right) = 0$ alors l'inégalité est trivialement vérifiée et si ce n'est pas le cas alors,
   $\ln\left(\mathbb{P}\left(\bigcap_{k=n}^{n+p} \overline{A_k}\right)\right) = \sum_{k=n}^{n+p} \ln(\mathbb{P}(\overline{A_k})) \leq \sum_{k=n}^{n+p} \left(\mathbb{P}(\overline{A_k}) - 1\right) = -\sum_{k=n}^{n+p} \mathbb{P}(A_k)$.
   Donc par passage à l'exponentielle qui est une fonction croissante sur $\mathbb{R}$,
   $\mathbb{P}\left(\bigcap_{k=n}^{n+p} \overline{A_k}\right) \leq \exp\left(-\sum_{k=n}^{n+p} \mathbb{P}(A_k)\right)$.

3. $\sum_{n\in\mathbb{N}} \mathbb{P}(A_n)$ étant une série à termes positifs divergente, sa somme vaut $+\infty$. Ainsi en faisant tendre p vers l'infini dans l'inégalité précédente, $\lim_{p\to+\infty} \mathbb{P}\left(\bigcap_{k=n}^{n+p} \overline{A_k}\right) \leq \exp\left(-\sum_{k=n}^{+\infty} \mathbb{P}(A_k)\right) = 0$. De plus par continuité décroissante, $\lim_{p\to+\infty} \mathbb{P}\left(\bigcap_{k=n}^{n+p} \overline{A_k}\right) = \lim_{p\to+\infty} \mathbb{P}\left(\bigcap_{k=n}^{+\infty} \overline{A_k}\right) = \mathbb{P}(\overline{B_n})$. Donc $\mathbb{P}(\overline{B_n}) = 0$.
   Ainsi comme $\mathbb{P}(\overline{A}) = \mathbb{P}\left(\bigcup_{n\in\mathbb{N}} \overline{B_n}\right) \leq \sum_{n=0}^{+\infty} \mathbb{P}(\overline{B_n}) = 0$, $\mathbb{P}(\overline{A}) = 0$ c'est à dire $\mathbb{P}(A) = 1$.

XIII.9.8 Formule d'antirépartition ★★★

[Enoncé]
Soit $N \in \mathbb{N}^*$.

$$\begin{aligned}\sum_{n=0}^{N} n\mathbb{P}(X=n) &= \sum_{n=1}^{N} n(\mathbb{P}(X>n-1)-\mathbb{P}(X>n)) \\ &= \sum_{n=1}^{N}((n-1)\mathbb{P}(X>n-1)-n\mathbb{P}(X>n)) + \sum_{n=1}^{N}\mathbb{P}(X>n-1) \\ &= \sum_{n=1}^{N}\mathbb{P}(X>n-1) - N\mathbb{P}(X>N) \\ &= \sum_{n=0}^{N-1}\mathbb{P}(X>n) - N\mathbb{P}(X>N)\end{aligned}$$

Si $\sum_{n\in\mathbb{N}}\mathbb{P}(X>n)$ converge alors $\forall N\in\mathbb{N}^*$, $\sum_{n=0}^{N} n\mathbb{P}(X=n) \leq \sum_{n=0}^{N-1}\mathbb{P}(X>n) \leq \sum_{n=0}^{+\infty}\mathbb{P}(X>n) < +\infty$ d'où X est d'espérance finie.
Réciproquement, supposons que X soit d'espérance finie.
Alors le reste $\sum_{n=N}^{+\infty} n\mathbb{P}(X=n)$ est défini et converge vers 0. De plus,
$\forall N\in\mathbb{N}$, $\sum_{n=N}^{+\infty} n\mathbb{P}(X=n) \geq N\sum_{n=N}^{+\infty}\mathbb{P}(X=n) = N\mathbb{P}(X>N) \geq 0$.
Donc $N\mathbb{P}(X>N) \underset{N\to+\infty}{\longrightarrow} 0$ et donc $\sum_{n=0}^{N-1}\mathbb{P}(X>n) \underset{\mathbb{N}\to+\infty}{\longrightarrow} \mathbb{E}(X) < +\infty$.

XIII.9.9 Loi de Poisson ★★

[Enoncé]

1. Soit $n\in\mathbb{N}$. Le choix du guichet pour une voiture étant aléatoire et indépendant des autres voitures, on suppose que la loi de X conditionnée par l'évènement $\{N=n\}$ est une loi binomiale de paramètre n et $p=\dfrac{1}{m}$.
   C'est à dire $\forall k\in[\![0;n]\!]$, $\mathbb{P}(X=k|N=n) = \binom{n}{k}\dfrac{1}{m^k}\left(1-\dfrac{1}{m}\right)^{n-k}$.
2. $N(\Omega)=\mathbb{N}$ donc d'après la formule des probabilités totales,
   $\mathbb{P}(X=k) = \sum_{n=0}^{+\infty}\mathbb{P}(N=n)\mathbb{P}(X=k|N=n) = \sum_{n=0}^{+\infty} e^{-\lambda}\dfrac{\lambda^n}{n!}\binom{n}{k}\dfrac{1}{m^k}\left(1-\dfrac{1}{m}\right)^{n-k} =$

$$e^{-\lambda}\left(\frac{\lambda}{m}\right)^k \frac{1}{k!}\sum_{n=k}^{+\infty}\frac{\lambda^{n-k}}{(n-k)!}\left(1-\frac{1}{m}\right)^{n-k}$$

D'où $\mathbb{P}(X=k)=\dfrac{e^{-\lambda}}{k!}\left(\dfrac{\lambda}{m}\right)^k\sum_{n=0}^{+\infty}\dfrac{\lambda^n}{n!}\left(1-\dfrac{1}{m}\right)^n$.

3. $X(\Omega)=\mathbb{N}$ et $\forall k\in\mathbb{N},\ \mathbb{P}(X=k)=\dfrac{e^{-\lambda}}{k!}\left(\dfrac{\lambda}{m}\right)^k e^{\lambda\left(1-\frac{1}{m}\right)}=e^{\frac{\lambda}{m}}\dfrac{\left(\frac{\lambda}{m}\right)^k}{k!}$: $X\sim\mathcal{P}\left(\dfrac{\lambda}{m}\right)$.
4. D'après le cours, $\mathbb{E}(X)=\mathbb{V}(X)=\dfrac{\lambda}{m}$.

XIII.9.10 Maximum de deux lois géométriques indépendantes ★

[Enoncé]

1. $M(\Omega)=\mathbb{N}^*\cup\{+\infty\}$. Fixons $k\in\mathbb{N}^*$.
   $\{M>k\}=\{X>k\}\cap\{Y>k\}$. Donc par indépendance $\mathbb{P}(M>k)=\mathbb{P}(X>k)\mathbb{P}(Y>k)$
   De plus $\mathbb{P}(X>k)=\sum_{i=k+1}^{+\infty}\mathbb{P}(X=i)=\sum_{i=k+1}^{+\infty}p(1-p)^{i-1}=p\cdot\dfrac{(1-p)^k}{1-(1-p)}=(1-p)^k$.
   De même, $\mathbb{P}(Y>k)=(1-q)^k$.
   D'après la formule d'antirépartition,

$$\begin{aligned}\mathbb{E}(M)&=\sum_{k=0}^{+\infty}\mathbb{P}(M>k)\\&=\sum_{k=0}^{+\infty}\mathbb{P}(X>k)\mathbb{P}(Y>k)\\&=\sum_{k=0}^{+\infty}[(1-p)(1-q)]^k\\&=\frac{1}{1-(1-p)(1-q)}\\&=\frac{1}{p+q-pq}\end{aligned}$$

2. <u>$1^{ère}$ méthode :</u> On utilise la question 1 :

   On a $Z+M=X+Y$ donc $\mathbb{E}(Z)=\mathbb{E}(X)+\mathbb{E}(Y)-\mathbb{E}(M)=\dfrac{1}{p}+\dfrac{1}{q}-\dfrac{1}{p+q-pq}$.

   <u>2^{nd} méthode :</u> On peut faire comme pour la question 1 :

   $Z(\Omega)=\mathbb{N}^*\cup\{+\infty\}$. Fixons $k\in\mathbb{N}^*$.

$\{Z \leq k\} = \{X \leq k\} \cap \{Y \leq k\}$. Donc par indépendance $\mathbb{P}(Z \leq k) = \mathbb{P}(X \leq k)\mathbb{P}(Y \leq k)$

De plus $\mathbb{P}(X \leq k) = \sum_{i=1}^{k} \mathbb{P}(X = i) = \sum_{i=1}^{k} p(1-p)^{i-1} = p \cdot \frac{1-(1-p)^k}{1-(1-p)} = 1-(1-p)^k$.

De même, $\mathbb{P}(Y \leq k) = 1-(1-q)^k$.

D'après la formule d'antirépartition,

$$\begin{aligned}
\mathbb{E}(Z) &= \sum_{k=0}^{+\infty} \mathbb{P}(Z > k) \\
&= \sum_{k=0}^{+\infty} (1 - \mathbb{P}(Z \leq k)) \\
&= \sum_{k=0}^{+\infty} (1 - \mathbb{P}(X \leq k)\mathbb{P}(Y \leq k)) \\
&= \sum_{k=0}^{+\infty} \left(1 - (1-(1-p)^k)(1-(1-q)^k)\right) \\
&= \sum_{k=0}^{+\infty} \left((1-p)^k + (1-q)^k - [(1-p)(1-q)]^k\right) \\
&= \sum_{k=0}^{+\infty} (1-p)^k + \sum_{k=0}^{+\infty} (1-q)^k - \sum_{k=0}^{+\infty} \left((1-p)(1-q)\right)^k \\
&= \frac{1}{p} + \frac{1}{q} - \frac{1}{1-(1-p)(1-q)} \\
&= \frac{1}{p} + \frac{1}{q} - \frac{1}{p+q-pq}
\end{aligned}$$

XIII.9.11 Max et min de lois géométriques iid ★★★★

[Enoncé]

1. Fixons $n \in \mathbb{N}^*$.
   Tout d'abord, $Y_n(\Omega) = \mathbb{N}^* \cup \{+\infty\}$.
   $\forall k \in \mathbb{N}^*,\ \{Y_n > k\} = \bigcap_{i=1}^{n} \{X_i > k\}$.
   Donc $\forall k \in \mathbb{N}^*, \mathbb{P}(Y_n > k) = \prod_{i=1}^{n} \mathbb{P}(X_i > k) = \prod_{i=1}^{n} (1-p)^k = (1-p)^{kn}$. Ainsi d'après la formule d'antirépartition,
   $\mathbb{E}(Y_n) = \sum_{k=0}^{+\infty} \mathbb{P}(Y_n > k) = \sum_{k=0}^{+\infty} (1-p)^{kn} = \frac{1}{1-(1-p)^n}$.

2. Fixons $n \in \mathbb{N}^*$.
Tout d'abord, $Z_n(\Omega) = \mathbb{N}^* \cup \{+\infty\}$.
D'après la formule d'antirépartition,

$$\begin{aligned}
\mathbb{E}(Z_n) &= \sum_{k=0}^{+\infty} \mathbb{P}(Z_n > k) \\
&= \sum_{k=0}^{+\infty} 1 - \mathbb{P}(Z_n \leq k) \\
&= \sum_{k=0}^{+\infty} 1 - \mathbb{P}\left(\bigcap_{i=1}^{n} \{X_i \leq k\}\right) \\
\text{(par indépendance)} \quad &= \sum_{k=0}^{+\infty} \left(1 - \prod_{i=1}^{n} \mathbb{P}(X_i \leq k)\right) \\
&= \sum_{k=0}^{+\infty} \left(1 - \prod_{i=1}^{n} (1 - \mathbb{P}(X_i > k))\right) \\
\text{avec } q = 1-p \quad &= \sum_{k=0}^{+\infty} \left(1 - \prod_{i=1}^{n} (1 - q^k)\right) \\
&= \sum_{k=0}^{+\infty} \left(1 - (1-q^k)^n\right)
\end{aligned}$$

Posons $f_n : \left\{ \begin{array}{ccc} \mathbb{R}_+ & \longrightarrow & \mathbb{R} \\ x & \longmapsto & 1-(1-q^x)^n \end{array} \right.$. f_n est continue décroissante et positive sur $\mathbb{R}_+$.

$$\begin{aligned}
&\forall k \in \mathbb{N}^* \ (x \in [k, k+1] \implies f_n(k+1) \leq f_n(x) \leq f_n(k)) \\
&\implies \sum_{k=0}^{+\infty} f_n(k+1) \leq \int_0^{+\infty} f(x)dx \leq \sum_{k=0}^{+\infty} f_n(k) \\
&\implies \mathbb{E}(Z_n) - f_n(0) \leq \int_0^{+\infty} f_n(x)dx \leq \mathbb{E}(Z_n) \\
&\implies \int_0^{+\infty} f_n(x)dx \leq \mathbb{E}(Z_n) \leq 1 + \int_0^{+\infty} f_n(x)dx
\end{aligned}$$

Calcul de $\displaystyle\int_0^{+\infty} f_n(x)dx$:
On pose $u = 1-q^x$. Ce changement de variable est légitime car la fonction $x \mapsto 1-q^x$ est de classe $\mathcal{C}^1$ et strictement décroissante sur $\mathbb{R}_+$.
$\displaystyle\int_0^{+\infty} f_n(x)dx = \int_0^1 (1-u^n)\frac{-du}{\ln(q)(1-u)} = -\frac{1}{\ln(q)}\int_0^1 \frac{1-u^n}{1-u}du = -\frac{1}{\ln(q)}\int_0^1 \sum_{k=0}^{n-1} u^k du =$

$$-\frac{1}{\ln(q)}\sum_{k=1}^{n}\frac{1}{k}$$ Ainsi, $\mathbb{E}(Z_n) \underset{n\to+\infty}{\sim} -\frac{\ln(n)}{\ln(q)} = -\log_q(n)$.

XIII.9.12 Formule de Wald ★★★

[Enoncé]

1. $S(\Omega) = \mathbb{N}$ est dénombrable. Soit $n \in \mathbb{N}$.
   $\{S = n\} = \bigsqcup_{p\in\mathbb{N}^*}\left(\{N = p\} \cap \left\{\sum_{k=1}^{p} X_k = n\right\}\right)$.
   Par opération, pour tout $p \in \mathbb{N}^*$ $S_p = \sum_{k=1}^{p} X_k$ est une variable aléatoire donc $\forall p, \in \mathbb{N}^*$ $\{S_p = n\} \in \mathcal{A}$.
   $\forall p \in \mathbb{N}^*$, $\{N = p\} \in \mathcal{A}$. La tribu est stable par intersection finie donc $\forall p \in \mathbb{N}^*$, $\{N = p\} \cap \{S_p = n\} \in \mathcal{A}$.
   Enfin, la tribu est stable par union dénombrable donc $\{S = n\} = \bigsqcup_{p\in\mathbb{N}^*}(\{N = p\}\cap\{S_p = n\}) \in \mathcal{A}$.
   S est bien une variable aléatoire discrète.

2. Soit $t \in [0, 1]$. Si $p \in \mathbb{N}^*$, $N, X_1, \dots, X_p$ sont mutuellement indépendantes donc d'après le lemme des coalitions, N et S_p sont indépendantes. On en déduit que $\forall n \in \mathbb{N}$, $\mathbb{P}(S = n) = \sum_{p=1}^{+\infty}\mathbb{P}(N = p)\mathbb{P}(S_p = n)$:
   $G_S(t) = \sum_{n=0}^{+\infty}\mathbb{P}(S = n)t^n = \sum_{n=0}^{+\infty}\sum_{p=1}^{+\infty}\mathbb{P}(N = p)\mathbb{P}(S_p = n)t^n$.
   $(\mathbb{P}(N = p)\mathbb{P}(S_p = n))_{(n,p)\in\mathbb{N}\times\mathbb{N}^*}$ est sommable puisque
   $\sum_{(n,p)\in\mathbb{N}\times\mathbb{N}^*}|\mathbb{P}(N = p)\mathbb{P}(S_p = n)t^n| = \sum_{n=0}^{+\infty}\sum_{p=1}^{+\infty}\mathbb{P}(N = p)\mathbb{P}(S_p = n)|t|^n = \sum_{n=0}^{+\infty}\mathbb{P}(S = n)|t|^n = G_S(|t|) < +\infty$.

   Alors d'après le théorème de Fubini,
   $G_S(t) = \sum_{p=1}^{+\infty}\sum_{n=0}^{+\infty}\mathbb{P}(N = p)\mathbb{P}(S_p = n)t^n = \sum_{p=1}^{+\infty}\mathbb{P}(N = p)\left(\sum_{n=0}^{+\infty}\mathbb{P}(S_p = n)t^n\right) = \sum_{p=1}^{+\infty}\mathbb{P}(N = p)G_{S_p}(t)$.
   Or pour tout $p \in \mathbb{N}^*$, $X_1, \dots, X_p$ sont mutuellement indépendantes. Donc $\forall p \in \mathbb{N}^*$, $G_{S_p}(t) = \prod_{k=1}^{p} G_{X_k}(t) = \prod_{k=1}^{p} G_X(t) = G_x(t)^p$.

Ainsi, $G_S(t) = \sum_{p=1}^{+\infty} \mathbb{P}(N=p) G_X(t)^p = G_N \circ G_X(t)$.

3. G_X est dérivable en 1 et G_N est dérivable en $G_X(1) = 1$ donc G_S est dérivable en 1 et,
$\mathbb{E}(S) = G_S'(1) = G_X'(1) \cdot G_N' \circ G_X(1) = \mathbb{E}(X)\mathbb{E}(N)$
4. G_X est deux fois dérivable en 1 et G_N est deux fois dérivable en $G_X(1) = 1$ donc G_S est deux fois dérivable en 1 et,

$$\begin{aligned}\mathbb{V}(S) &= G_S''(1) + G_S'(1) - G_S'(1)^2 \\ &= G_X''(1) \cdot G_N' \circ G_X(1) + G_X'(1)^2 \cdot G_N'' \circ G_X(1) + \mathbb{E}(S) - \mathbb{E}(S)^2 \\ &= (\mathbb{V}(X) + \mathbb{E}(X)^2 - \mathbb{E}(X))\mathbb{E}(N) + \mathbb{E}(X)^2(\mathbb{V}(N) + \mathbb{E}(N)^2 - \mathbb{E}(N)) + \mathbb{E}(X)\mathbb{E}(N) - \mathbb{E}(X)^2 \\ &= \mathbb{V}(X)\mathbb{E}(N) + \mathbb{E}(X)^2\mathbb{V}(N)\end{aligned}$$

XIII.9.13 Loi binomiale aléatoire ★★★

[Enoncé]
Tout d'abord, $Y(\Omega) = \mathbb{N}$ est dénombrable. Fixons $k \in \mathbb{N}$.
$\{Y = k\} = \bigsqcup_{n\in\mathbb{N}} (\{N = n\} \cap \{X_n = k\})$.
$\forall n \in \mathbb{N},\ (\{N = n\}, \{X_n = k\}) \in \mathcal{A}^2$. La tribu est stable par intersection finie et par réunion dénombrable donc $\{Y = k\} \in \mathcal{A}$.
Ainsi Y est bien une variable aléatoire discrète.
De plus par indépendance, $\forall n \in \mathbb{N},\ \mathbb{P}(N = n, X_n = k) = \mathbb{P}(N+1 = n+1)\mathbb{P}(X_n = k) = q(1-q)^n \binom{n}{k} p^k (1-p)^{n-k}$.
Donc,

$$\begin{aligned}\mathbb{P}(Y = k) &= \sum_{n=0}^{+\infty} \mathbb{P}(N = n, X_n = k) \\ &= q(p(1-q))^k \sum_{n=0}^{+\infty} \binom{n}{k} ((1-p)(1-q))^{n-k} \\ &= \frac{q(p(1-q))^k}{k!} \sum_{n=k}^{+\infty} \frac{n!}{(n-k)!} ((1-p)(1-q))^{n-k}\end{aligned}$$

On reconnaît la somme de la dérivée k-ième de la série géométrique en $(1-p)(1-q) \in]-1, 1[$:
$\sum_{n=k}^{+\infty} \frac{n!}{(n-k)!} x^{n-k} = \frac{d^k}{dx^k}\left(\sum_{n=0}^{+\infty} x^n\right) = \frac{d^k}{dx^k}\left(\frac{1}{1-x}\right) = \frac{k!}{(1-x)^{k+1}}$
Donc, $\mathbb{P}(Y = k) = \frac{q(p(1-q))^k}{k!} \sum_{n=k}^{+\infty} \frac{n!}{(n-k)!} ((1-p)(1-q))^{n-k} = q\frac{(p(1-q))^k}{(p+q-pq)^{k+1}} =$

$\frac{q}{p+q-pq}\left(1-\frac{q}{p+q-pq}\right)^k$.
$Y \sim \mathcal{G}\left(\frac{q}{p+q-pq}\right)$.

XIII.9.14 Somme de lois de Poisson ★

[Enoncé]

$\forall t \in [-1,1],\ G_S(t) = \mathbb{E}(t^S) = \mathbb{E}\left(\prod_{i=1}^{n} t^{X_i}\right)$.

Et par indépendance, $\forall t \in [-1,1],\ \mathbb{E}\left(\prod_{i=1}^{n} t^{X_i}\right) = \prod_{i=1}^{n} \mathbb{E}\left(t^{X_i}\right) = \prod_{i=1}^{n} G_{X_i}(t) = \prod_{i=1}^{n} e^{(t-1)\lambda_i} = e^{(t-1)\sum_{i=1}^{n}\lambda_i}$.

Ainsi $S \sim \mathcal{P}\left(\sum_{i=1}^{n}\lambda_i\right)$.

XIII.9.15 Obtenir trois pile consécutifs

[Enoncé]

XIII.9.16 Lancer de dés équitable ★★★

[Enoncé]

Supposons que $X \sim \mathcal{U}([\![2;12]\!])$. Notons D_1 et D_2 les variables aléatoire qui donnent le résultat des dés 1 et 2 respectivement de sorte que $X = D_1 + D_2$. D'après l'énoncé, D_1 et D_2 sont indépendantes. Fixons $t \in]-1,1[$.

$G_X(t) = \sum_{k=2}^{12} \frac{1}{11} t^k = \frac{t^2}{11} \cdot \frac{t^{11}-1}{t-1}$. Or par indépendance, $G_X(t) = G_{D_1}(t) G_{D_2}(t)$.

Notons $G_{D_1}(t) = \sum_{k=1}^{6} p_k t^k$ et $G_{D_1}(t) = \sum_{k=1}^{6} q_k t^k$.

$\forall t \in]-1,1[\backslash\{0\},\ G_X(t) = G_{D_1}(t)G_{D_2}(t) \implies \frac{1}{11} \cdot \frac{t^{11}-1}{t-1} = \left(\sum_{k=0}^{5} p_{k+1} t^k\right)\left(\sum_{k=0}^{5} q_{k+1} t^k\right)$.

$\sum_{k=0}^{5} p_{k+1} t^k$ est un polynôme à coefficients réels de degré impair, il admet donc une racine réelle. Cependant, les racines de G_X sont les racines 11-ième de l'unité hormis 1, il n'a donc aucune racine réelle.

Ceci est absurde, par conséquent il est impossible de truquer les deux dés de manière à ce que $X \sim \mathcal{U}([\![2;12]\!])$.

XIII.9.17 Espérance conditionnelle ★★★

[Enoncé]

1. $\forall x \in X(\Omega),\ \{X=x\} \cap A \subset \{X=x\}$.
   Donc $\forall x \in X(\Omega),\ |\mathbb{P}(\{X=x\} \cap A)| = \mathbb{P}(\{X=x\} \cap A) \leq \mathbb{P}(X=x) = |\mathbb{P}(X=x)|$.
   La famille $(x\mathbb{P}(X=x))_{x\in X(\Omega)}$ est sommable par hypothèse donc $(x\mathbb{P}_A(X=x))_{x\in X(\Omega)} = \left(\dfrac{x\mathbb{P}(X=x)}{\mathbb{P}(A)}\right)_{x\in X(\Omega)}$ est sommable.
   Fixons $x \in X(\Omega)\backslash\{0\}$. On sait que $\mathbb{1}_A \sim \mathcal{B}(\mathbb{P}(A))$ donc $\forall \omega \in \Omega,\ (\mathbb{1}_A \cdot X)(\omega) = 1 \iff \mathbb{1}_A(\omega)X(\omega) = 1 \iff (\mathbb{1}_A(\omega) = 1 \wedge X(\omega) = x) \iff \omega \in A \cap \{X=x\}$.
   Ainsi, $\forall x \in X(\Omega)\backslash\{0\},\ \mathbb{P}_A(X=x) = \dfrac{\mathbb{P}(\{X=x\}\cap A)}{\mathbb{P}(A)} = \dfrac{\mathbb{P}(\mathbb{1}_A \cdot X = x)}{\mathbb{P}(A)}$.
   Et $\mathbb{E}(\mathbb{1}_A \cdot X) = \displaystyle\sum_{x\in X(\Omega)\cup\{0\}} x\mathbb{P}(\mathbb{1}_A \cdot X = x) = \sum_{x\in X(\Omega)\backslash\{0\}} x\mathbb{P}(\mathbb{1}_A \cdot X = x) = \mathbb{P}(A) \sum_{x\in X(\Omega)\backslash\{0\}} x\mathbb{P}_A(X = x) = \mathbb{P}(A)\mathbb{E}_A(X)$.

   C'est à dire, $\mathbb{E}_A(X) = \dfrac{\mathbb{E}(\mathbb{1}_A \cdot X)}{\mathbb{P}(A)}$.
2. D'après la formule des probabilités totales, $\forall x \in X(\Omega),\ \mathbb{P}(X=x) = \displaystyle\sum_{i\in I} \mathbb{P}_{A_i}(X = x)\mathbb{P}(A_i)$.
   La famille $(x\mathbb{P}_{A_i}(X=x)\mathbb{P}(A_i))_{(x,i)\in X(\Omega)\times I}$ est sommable. En effet, $\displaystyle\sum_{(x,i)\in X(\Omega)\times I} |x\mathbb{P}_{A_i}(X=x)\mathbb{P}(A_i)| = \sum_{x\in X(\Omega)} |x| \sum_{i\in I} \mathbb{P}_{A_i}(X=x)\mathbb{P}(A_i) = \sum_{x\in X(\Omega)} |x\mathbb{P}(X = x)| < +\infty$ par hypothèse.

   Par conséquent d'après le théorème de Fubini,
   $\mathbb{E}(X) = \displaystyle\sum_{x\in X(\Omega)} x\mathbb{P}(X=x) = \sum_{x\in X(\Omega)} \sum_{i\in I} x\mathbb{P}_{A_i}(X=x)\mathbb{P}(A_i) = \sum_{i\in I} \mathbb{P}(A_i) \sum_{x\in X(\Omega)} x\mathbb{P}_{A_i}(X = x) = \sum_{i\in I} \mathbb{E}_{A_i}(X)\mathbb{P}(A_i)$.

XIII.9.18 Problème du collectionneur ★★

[Enoncé]

1. $X_{n,i}(\Omega) = \mathbb{N}^*$.
   $X_{n,i}$ est la variable aléatoire qui donne le rang du premier succès de l'expérience de Bernoulli "acheter une carte et regarder si on l'a déjà" lorsque que l'on la répète de

manière indépendante. On suppose que la répartition des n cartes est uniforme au cours de tous les achats donc la probabilité du succès de cette expérience aléatoire est $\frac{n-i+1}{n}$. Alors $X_{n,i}$ suit une loi géométrique de paramètre $\frac{n-i+1}{n}$.
On sait alors que

$$\mathbb{E}(X_{n,i}) = \frac{n}{n-i+1} \text{ et } \mathbb{V}(X) = \frac{1-\frac{n-i+1}{n}}{\left(\frac{n-i+1}{n}\right)^2} = \frac{n(i-1)}{(n-i+1)^2}$$

. Ces expressions sont encore valables pour $i = 1$.

2. Pour tout $i \in [\![1; n]\!]$, l'expérience aléatoire associée à $X_{n,i}$ n'est pas impactée par les valeurs prises par $X_{n,1}, \dots, X_{n,i-1}$. On peut donc supposer que $X_{n,1}, \dots, X_{n,n}$ sont mutuellement indépendantes.

3. Par linéarité de l'espérance,
$\mathbb{E}(T_n) = \sum_{i=1}^{n} \mathbb{E}(X_{n,i}) = n\sum_{i=1}^{n} \frac{1}{n-i+1} = n\sum_{i=1}^{n} \frac{1}{i} = nH_n$.
Comme $X_{n,1}, \dots, X_{n,n}$ sont mutuellement indépendantes,
$\mathbb{V}(T_n) = \sum_{i=1}^{n} \mathbb{V}(X_{n,i}) = n\sum_{i=1}^{n} \left(\frac{n}{(n-i+1)^2} - \frac{n-i+1}{(n-i+1)^2}\right) = n^2\sum_{i=1}^{n} \frac{1}{i^2} - n\sum_{i=1}^{n} \frac{1}{i} = n^2 S_n - nH_n$.
$\frac{1}{n} \underset{n\to+\infty}{\sim} \ln\left(1+\frac{1}{n}\right) = \ln(n+1) - \ln(n)$.
$\sum_{n\in\mathbb{N}^*} \frac{1}{n}$ diverge et $\forall n \in \mathbb{N}^*,\ \frac{1}{n} \geq 0$ donc d'après les théorèmes de comparaison pour des séries divergentes,
$H_n \underset{n\to+\infty}{\sim} \sum_{k=1}^{n} (\ln(k+1) - \ln(k)) = \ln(n+1) = \ln(n) + \ln\left(1+\frac{1}{n}\right) \underset{n\to+\infty}{\sim} \ln(n)$.
$\sum_{n=1}^{+\infty} \frac{1}{n^2}$ converge donc sa somme partielle est équivalente à sa somme $S = \frac{\pi^2}{6}$. (Il n'est pas nécessaire d'avoir la valeur de S)
Ainsi, $\mathbb{E}(T_n) \underset{n\to+\infty}{\sim} n\ln n$ et $\mathbb{V}(T_n) \underset{n\to+\infty}{\sim} \frac{\pi^2}{6}n^2 - n\ln n \underset{n\to+\infty}{\sim} \frac{\pi^2}{6}n^2$.

Généralisation

1. $\mathbb{E}(R_n) = \sum_{(x_1,\dots,x_n)\in X(\Omega)^n} \text{Card}(\{x_1,\dots,x_n\})\mathbb{P}(X=x_1,\dots,X_n=x_n) = \sum_{(x_1,\dots,x_n)\in X(\Omega)^n} \text{Card}(\{x_1,\dots,x_k) \leq$

   $$\begin{aligned}\mathbb{E}(R_{n+1}) &= \sum_{(x_1,\dots,x_n,x_{n+1})\in\mathbb{N}^{n+1}} \text{Card}(\{x_1,\dots,x_n,x_{n+1}\})\mathbb{P}(X_1=x_1,\dots,X_n=x_n,X_{n+1}=x_{n+1}) \\ &\leq \sum_{k=0}^{+\infty}\sum_{(x_1,\dots,x_n)\in\mathbb{N}^n} (\text{Card}(\{x_1,\dots,x_n\})+1)\mathbb{P}(X_1=x_1,\dots,X_n=x_n)\mathbb{P}(X_{n+1}=k) \\ &= \sum_{k=0}^{+\infty}\mathbb{P}(X_{n+1}=k)(\mathbb{E}(R_n)+1) \\ &= \mathbb{E}(R_n)+1 \\ &\leq a+1+n\mathbb{P}(X\geq a)\end{aligned}$$

XIII.9.19 Problème de la ruine du joueur

[Enoncé]

XIII.9.20 Passager d'un avion

[Enoncé]

XIII.9.21 Fonction de répartition ★★★★

[Enoncé]
On sait que $X(\Omega)$ est au plus dénombrable.
S'il est fini on note $X(\Omega) = \{x_1,\dots,x_n\}$.
S'il est dénombrable on pose une bijection $S : \left\{\begin{array}{ccc}\mathbb{N} & \longrightarrow & X(\Omega) \\ n & \longmapsto & s_n\end{array}\right.$.

1. Soient $x, y \in \mathbb{R}$ tels que $x \leq y$.
   $\{X\leq x\} \subset \{X\leq y\}$ donc $F_X(x) = \mathbb{P}(X\leq x) \leq \mathbb{P}(X\leq y) = F_X(y)$.
   De plus, $\forall x\in\mathbb{R},\ 0\leq F_X(x)\leq 1$. Donc d'après le théorème de la limite monotone F_X admet des limites en $\pm\infty$.
   Déterminons les limites de F_X.
   Si $X(\Omega)$ est fini :
   On note $m = \min(X(\Omega))$ et $M = \max(X(\Omega))$. $(\forall x<m,\ F_X(x)=0) \implies \lim\limits_{x\to-\infty} F_X(x) = 0$.
   $(\forall x\geq M,\ F_X(x)=1) \implies \lim\limits_{x\to+\infty} F_X(x) = 1$.

Si $X(\Omega)$ est dénombrable :
1ère méthode : Continuité (dé)croissante.
Notons pour $k \in \mathbb{Z}$, $A_k = \{X \leq k\}$. $(A_k)_{k\in\mathbb{N}}$ est une suite croissante d'évènement. Par continuité croissante,

$$\lim_{x\to+\infty} F_X(x) = \lim_{n\to+\infty} \mathbb{P}(A_k) = \mathbb{P}\left(\bigcup_{k\in\mathbb{N}} A_k\right) = \mathbb{P}(X \leq +\infty) = 1.$$

Similairement, $(A_{-k})_{k\in\mathbb{N}}$ est une suite décroissante d'évènement. Par continuité décroissante,

$$\lim_{x\to-\infty} F_X(x) = \lim_{n\to+\infty} \mathbb{P}(A_{-k}) = \mathbb{P}\left(\bigcap_{k\in\mathbb{N}} A_{-k}\right) = \mathbb{P}(X \leq -\infty) = 0.$$

2nd méthode : Série de fonctions.
On remarque que $\forall x \in \mathbb{R},\ F_X(x) = \sum_{s\in X(\Omega)} \mathbb{P}(X = s)\mathbb{1}_{[s,+\infty[}(x)$. Si $x \in \mathbb{R}$, comme $(\mathbb{P}(X = s)\mathbb{1}_{[s,+\infty[}(x))_{s\in X(\Omega)}$ est une famille positive on a $\sum_{s\in X(\Omega)} \mathbb{P}(X = s)\mathbb{1}_{[s,+\infty[}(x) = \sum_{n\in\mathbb{N}} \mathbb{P}(X = s_n)\mathbb{1}_{[s_n,+\infty[}(x)$.
Posons pour $n \in \mathbb{N}$, $f_n = \mathbb{P}(X = s_n)\mathbb{1}_{[s_n,+\infty[}$.

- $\sum_{n\in\mathbb{N}} f_n$ converge normalement, a fortiori uniformément sur $\mathbb{R}$.
  En effet, $\sum_{n=0}^{+\infty} ||f_n||_\infty = \sum_{n=0}^{+\infty} \mathbb{P}(X = s_n) = 1$;
- $\forall n \in \mathbb{N},\ f_n(x) \underset{x\to+\infty}{\longrightarrow} \mathbb{P}(X = s_n) \in \mathbb{R}$;
- $\forall n \in \mathbb{N},\ f_n(x) \underset{x\to-\infty}{\longrightarrow} 0 \in \mathbb{R}$.

Donc d'après le théorème d'interversion série-limite, $\lim_{x\to+\infty} F_X(x) = \sum_{n=0}^{+\infty} \mathbb{P}(X = s_n) = 1$ et $\lim_{x\to-\infty} F_X(x) = \sum_{n=0}^{+\infty} 0 = 0$.

3ème méthode : Par la définition
On remarque que $\forall x \in \mathbb{R},\ F_X(x) = \sum_{s\in X(\Omega)} \mathbb{P}(X = s)\mathbb{1}_{[s,+\infty[}(x)$. Soit $\varepsilon \in \mathbb{R}_+^*$.
$\sum_{n=0}^{+\infty} \mathbb{P}(X = s_n) = 1$ et $\left(\sum_{n=0}^{N} \mathbb{P}(X = s_n)\right)_{N\in\mathbb{N}}$ est croissante donc $\exists N \in \mathbb{N},\ \forall n > N,\ \sum_{n=0}^{N} \mathbb{P}(X = s_n) \geq 1 - \varepsilon$.
Soit $x \geq \max\{s_n,\ n \in [\![0; N]\!]\}$.

$(\forall n \in [\![0;N]\!],\ \mathbb{1}_{[s_n,+\infty[}(x)=1) \implies \sum_{n=0}^{+\infty}\mathbb{P}(X=s_n)\mathbb{1}_{[s_n,+\infty[}(x) \geq \sum_{n=0}^{N}\mathbb{P}(X=s_n) \geq 1-\varepsilon$

De plus, $\forall x \in \mathbb{R},\ \sum_{n=0}^{+\infty}\mathbb{P}(X=s_n)\mathbb{1}_{[s_n,+\infty[}(x) \leq \sum_{n=0}^{+\infty}\mathbb{P}(X=s_n)=1$

Ainsi, $\lim\limits_{x\to+\infty} F_X(x)=1$.

Ensuite, $\sum_{n\in\mathbb{N}}\mathbb{P}(X=s_n)$ converge donc la suite des restes $(R_p)_{p\in\mathbb{N}} = \left(\sum_{n=p+1}^{+\infty}\mathbb{P}(X=s_n)\right)_{p\in\mathbb{N}}$ converge vers 0. Alors, $\exists M\in\mathbb{N},\ \forall n>M,\ |R_p|=R_p\leq\varepsilon$.

Soit $x \leq \min\{s_n,\ n\in[\![0;M]\!]\}$.

$(\forall n\in[\![0;M]\!],\ \mathbb{1}_{[s_n,+\infty[}(x)=0) \implies \sum_{n=0}^{+\infty}\mathbb{P}(X=s_n)\mathbb{1}_{[s_n,+\infty[}(x) \leq R_M \leq \varepsilon$.

Ainsi, $\lim\limits_{x\to-\infty} F_X(x)=0$.

2. **Si $X(\Omega)$ est fini :**

$F_X = \sum_{k=1}^{n}\mathbb{P}(X=x_k)\mathbb{1}_{[x_k,+\infty[}$ donc F_X est continue à droite en tout point comme somme (finie) de fonctions continues à droite en tout point.

Si $X(\Omega)$ est dénombrable :

1ère méthode : Continuité (dé)croissante.

Soient $x\in\mathbb{R}$ et $(x_n)\in(]x,+\infty[)^{\mathbb{N}}$ convergeant vers x.

Montrons le lemme suivant : D'une suite réelle peut toujours être extraite une suite monotone.

Fixons $(u_n)\in\mathbb{R}^{\mathbb{N}}$ et posons $A=\{n\in\mathbb{N}|\forall k>n,\ u_k\geq u_n\}$. Alors,
soit A est infini et la suite $(u_n)_{n\in A}$ est une suite extraite de (u_n) croissante,
soit A est fini et il existe donc $N\in\mathbb{N},\ \forall n\geq N,\ n\notin A$. On construit alors l'extractrice par récurrence : $\varphi(0)=N$ puis, si $N=\varphi(0)<\cdots<\varphi(n)$ sont bien définis alors $\varphi(n)\notin A$ donne l'existence de $k>\varphi(n)$ tel que $u_k<u_{\varphi(n)}$. On pose donc $\varphi(n+1)=k$. Par définition, $(u_{\varphi(n)})_{n\in\mathbb{N}}$ est décroissante.

On applique le lemme a (x_n) pour extraire une suite (y_n) de (x_n) monotone. On remarque que si (y_n) est croissante alors comme elle converge vers x en tant que suite extraite, $\forall n\in\mathbb{N},\ y_n\leq x$. Or par définition de (x_n), $\forall n\in\mathbb{N},\ y_n>x$. Ceci est absurde par conséquent (y_n) est décroissante.

Mais alors $(\{X\leq y_n\})_{n\in\mathbb{N}}$ est une suite décroissante d'évènements d'où par continuité décroissante,

$\lim\limits_{n\to+\infty} F_X(x_n) = \lim\limits_{n\to+\infty} F_X(y_n) = \lim\limits_{n\to+\infty}\mathbb{P}(\{X\leq y_n\}) = \mathbb{P}\left(\bigcap_{k\in\mathbb{N}}\{X\leq y_k\}\right) = \mathbb{P}(X\leq x) = F_X(x)$.

F_X est continue à droite en x par caractérisation séquentielle.

2^{nd} méthode : Série de fonctions.
On réutilise l'expression $F_X = \sum_{n\in\mathbb{N}} \mathbb{P}(X = s_n)\mathbb{1}_{[s_n,+\infty[}$. On a déjà montré la convergence normale, et donc uniforme, sur $\mathbb{R}$ de la série $\sum_{n\in\mathbb{N}} \mathbb{P}(X = s_n)\mathbb{1}_{[s_n,+\infty[}$. De plus, quel que soit $n \in \mathbb{N}$, $\mathbb{P}(X = s_n)\mathbb{1}_{[s_n,+\infty[}$ est continue à droite en tout point de $\mathbb{R}$. Donc par théorème de transfert, F_X est continue à droite en tout point de $\mathbb{R}$.

3. **Si $X(\Omega)$ est fini :**
$F_X = \sum_{k=1}^{n} \mathbb{P}(X = x_k)\mathbb{1}_{[x_k,+\infty[}$ donc F_X est continue sur $\mathbb{R}\backslash X(\Omega)$ comme somme (finie) de fonctions continues sur $\mathbb{R}\backslash X(\Omega)$, et F_X est continue en un des points x_k, $k \in [\![1; n]\!]$ si et seulement si $\mathbb{P}(X = x = k) = 0$.
Si $X(\Omega)$ est dénombrable :
$1^{ère}$ méthode : Continuité (dé)croissante.
Soient $a \in \mathbb{R}$ et $(a_n) \in (]-\infty, x[)^{\mathbb{N}}$ convergeant vers a.
On applique le lemme démontré précédemment à (a_n) pour extraire une suite (b_n) de (a_n) monotone. On remarque pour des raisons analogues à celles de la question précédente que (b_n) est croissante.
Mais alors $(\{X \leq b_n\})_{n\in\mathbb{N}}$ est une suite croissante d'évènements d'où par continuité croissante,
$\lim_{n\to+\infty} F_X(a_n) = \lim_{n\to+\infty} F_X(b_n) = \lim_{n\to+\infty} \mathbb{P}(\{X \leq b_n\}) = \mathbb{P}\left(\bigcup_{k\in\mathbb{N}} \{X \leq b_k\}\right) = \mathbb{P}(X < a) = F_X(a) - \mathbb{P}(X = a)$.
Ainsi, F_X est continue en a si et seulement si $\mathbb{P}(X = a) = 0$ c'est à dire si et seulement si l'évènement $\{X = a\}$ est négligeable.

XIII.9.22 Loi sans mémoire ★★

[Enoncé]
Supposons que $X \sim \mathcal{G}(p)$ pour un certain $p \in]0, 1[$. On note $q = 1 - p$.
Alors $\forall m \in \mathbb{N}$, $\mathbb{P}(X > m) = \sum_{i=m+1}^{+\infty} pq^{i-1} = p \cdot \frac{q^m}{1-q} = q^m$.
Fixons $(n, k) \in \mathbb{N}^2$.
$\mathbb{P}(X > n + k|X > n) = \frac{\mathbb{P}(X > n + k, X > n)}{\mathbb{P}(X > n)} = \frac{\mathbb{P}(X > n + k)}{\mathbb{P}(X > n)} = \frac{q^{n+k}}{q^m} = q^k = \mathbb{P}(X > k)$.
Réciproquement, supposons que $\forall (n, k) \in \mathbb{N}^2$, $\mathbb{P}(X > n + k|X > n) = \mathbb{P}(X > k)$. Fixons $n \in \mathbb{N}$.
$\mathbb{P}(X > n+1) = \mathbb{P}(X > n+1, X > n) = \mathbb{P}(X > n)\mathbb{P}(X > n+1|X > n) = \mathbb{P}(X > n)\mathbb{P}(X > 1)$.
Ainsi, $(\mathbb{P}(X > n))_{n\in\mathbb{N}^*}$ est une suite géométrique de raison $\mathbb{P}(X > 1)$: $X \sim \mathcal{G}(\mathbb{P}(X > 1))$.

XIII.9.23 Caractérisation de la loi de Poisson par l'espérance

[Enoncé]

XIII.9.24 Loi Zéta ★★

[Enoncé]

1. On doit avoir $\sum_{n=1}^{+\infty}\mathbb{P}(X=n)=1$ donc $\lambda\sum_{n=1}^{+\infty}\frac{1}{n^s}=1$ c'est à dire $\lambda=\frac{1}{\zeta(s)}$.
2. Soit $n\in\mathbb{N}^*$.
   $\mathbb{P}(n|X)=\mathbb{P}(X\in n\mathbb{N}^*)=\mathbb{P}\left(X\in\bigsqcup_{m\in\mathbb{N}^*}\{mn\}\right)=\sum_{m=1}^{+\infty}\mathbb{P}(X=mn)=\zeta(s)^{-1}\sum_{m=1}^{+\infty}\frac{1}{(mn)^s}=$
   $\frac{\zeta(s)^{-1}}{n^s}\sum_{m=1}^{+\infty}\frac{1}{m^s}=\frac{1}{n^s}$.
3. Fixons $q\in\mathbb{N}^*$. Soient $i_1,\dots,i_q\in\mathbb{N}^*$ distincts.
   D'après le lemme d'Euclide, $\forall k\in\mathbb{N}^*,\ (\forall j\in[\![1;q]\!],\ p_{i_j}^{\alpha_{i_j}}|k)\iff\prod_{j=1}^{q}p_{i_j}^{\alpha_{i_j}}|k$.
   Donc $\bigcap_{j=1}^{q}\left\{p_{i_j}^{\alpha_{i_j}}|X\right\}=\left\{\prod_{j=1}^{q}p_{i_j}^{\alpha_{i_j}}|X\right\}$.
   On en déduit d'après la question précédente que $\mathbb{P}\left(\bigcap_{j=1}^{q}\left\{p_{i_j}^{\alpha_{i_j}}|X\right\}\right)=\left(\prod_{j=1}^{q}p_{i_j}^{\alpha_{i_j}}\right)^{-s}=$
   $\prod_{j=1}^{q}\left(p_{i_j}^{\alpha_{i_j}}\right)^{-s}=\prod_{j=1}^{q}\mathbb{P}\left(p_{i_j}^{\alpha_{i_j}}|X\right)$.
4. Les évènements $\{p_1|X\},\dots,\{p_r|X\}$ sont mutuellement indépendants donc,
   $\mathbb{P}\left(\bigcap_{i=1}^{r}\{p_i\nmid X\}\right)=\prod_{i=1}^{r}\mathbb{P}\left(\overline{p_i|X}\right)=\prod_{i=1}^{r}\left(1-p_i^{-s}\right)$.
5. Par continuité décroissante $\zeta(s)^{-1}=\mathbb{P}(X=1)=\mathbb{P}\left(\bigcap_{k=1}^{+\infty}\{p_k\nmid X\}\right)=\lim_{n\to+\infty}\mathbb{P}\left(\bigcap_{k=1}^{n}\{p_k\nmid X\}\right)$.
   Et donc d'après la question précédente, $\zeta(s)^{-1}=\lim_{n\to+\infty}\prod_{k=1}^{n}\mathbb{P}\left(p_k\nmid X\right)=\lim_{n\to+\infty}\prod_{k=1}^{n}\left(1-p_k^{-s}\right)$.
6. La famille $\left(\frac{1}{p}\right)_{p\in\mathcal{P}}$ est positive donc, dans $\mathbb{R}\cup\{+\infty\}$, $\sum_{p\in\mathcal{P}}\frac{1}{p}=\sum_{n=1}^{+\infty}\frac{1}{p_n}$.
   De plus, comme $p_n\underset{n\to+\infty}{\longrightarrow}+\infty$, $\frac{1}{p_n}\underset{n\to+\infty}{\sim}-\ln\left(1-\frac{1}{p_n}\right)$ et $\left(\frac{1}{p_n}\right)_{n\in\mathbb{N}^*}$ est positive

APCR. Donc $\sum_{n\in\mathbb{N}^*}\frac{1}{p_n}$ et $\sum_{n\in\mathbb{N}^*}-\ln\left(1-\frac{1}{p_n}\right)$ sont de même nature.

Supposons que $\left(\frac{1}{p}\right)_{p\in\mathcal{P}}$ est sommable. Alors d'après ce qui a été fait précédemment, $\sum_{n\in\mathbb{N}^*}-\ln\left(1-\frac{1}{p_n}\right)$ converge.

$\forall N\in\mathbb{N}^*,\ \sum_{n=1}^{N}\ln\left(1-\frac{1}{p_n}\right)=\ln\left(\prod_{n=1}^{N}\left(1-\frac{1}{p_n}\right)\right)$.

Donc la suite $(u_N)_{N\in\mathbb{N}^*}$ définit par $\forall N\in\mathbb{N}^*,\ u_n=\prod_{n=1}^{N}\left(1-\frac{1}{p_n}\right)$ converge. Notons l sa limite et fixons $N\in\mathbb{N}^*$. $\forall n\in[\![1;N]\!],\ 0\leq\frac{1}{p_n}<1$. Donc, $s>1\implies\forall n\in[\![1;N]\!],\ 1>\frac{1}{p_n}>\frac{1}{p_n^s}\geq 0\implies 0<1-\frac{1}{p_n}<1-p_n^{-s}\implies 0<u_N<\prod_{n=1}^{N}\left(1-p_n^{-s}\right)$.

Ainsi, par passage à la limite, $0\leq l\leq\zeta(s)^{-1}$.

On montre alors classiquement que $\lim_{s\to1^+}\zeta(s)=+\infty$ pour conclure que $l=0$ ce qui est absurde car alors $(\ln(u_n))_{n\in\mathbb{N}^*}=\sum_{n\in\mathbb{N}}\ln\left(1-\frac{1}{p_n}\right)$ diverge :

$t\mapsto t^{-s}$ est continue positive, décroissante sur $[1,+\infty[$ et intégrable en $+\infty$ donc,

$$\left(\forall n\in\mathbb{N}^*,\ \int_n^{n+1}t^{-s}dt\leq\frac{1}{n^s}\right)\wedge\left(\forall n\in[\![2;+\infty[\![,\ \frac{1}{n^s}\leq\int_{n-1}^{n}t^{-s}dt\right)$$

puis en sommant dans les deux inégalités,

$$\int_1^{+\infty}t^{-s}dt\leq\zeta(s)\leq1+\int_1^{+\infty}t^{-s}dt$$

c'est à dire,

$$\frac{1}{s-1}\leq\zeta(s)\leq1+\frac{1}{s-1}$$

Or, $\frac{1}{s-1}\underset{s\to1^+}{\sim}1+\frac{1}{s-1}$ donc $\zeta(s)\underset{s\to1^+}{\sim}\frac{1}{s-1}$ d'où $\lim_{s\to1^+}\zeta(s)=+\infty$.

XIII.9.25 Taux de panne ★★

[Enoncé]

1. $\sum_{n=1}^{+\infty}\frac{1}{n(n+1)}=\sum_{n=1}^{+\infty}\left(\frac{1}{n}-\frac{1}{n+1}\right)=1$ et $\forall n\in\mathbb{N}^*,\ \frac{1}{n(n+1)}\geq0$: $\left(\frac{1}{n(n+1)}\right)_{n\in\mathbb{N}^*}$ définit une loi de probabilité. Fixons $n\in\mathbb{N}^*$.

$$\mathbb{P}(Y=n|Y\geq n)=\frac{\mathbb{P}(Y=n,Y\geq n)}{\mathbb{P}(Y\geq n)}=\frac{\mathbb{P}(Y=n)}{\sum_{k=n}^{+\infty}\mathbb{P}(Y=k)}=\frac{\frac{1}{n(n+1)}}{\frac{1}{n}}=\frac{1}{n+1}.$$

2. Soit $n\in[\![2;+\infty[\![$. D'après la formule des probabilités totales,
$\forall k\in[\![1;n-1]\!],\ 1-x_k=1-\dfrac{\mathbb{P}(X=k)}{\mathbb{P}(X\geq k)}=\dfrac{\mathbb{P}(X\geq k+1)}{\mathbb{P}(X\geq k)}.$
Par conséquent, $\mathbb{P}(X\geq n)=\dfrac{\mathbb{P}(X\geq n)}{\mathbb{P}(X\geq 1)}=\prod_{k=1}^{n-1}(1-x_k).$

3. $\forall n\in[\![2;+\infty[\![,\ \mathbb{P}(X=n)=\mathbb{P}(X\geq n)-\mathbb{P}(X\geq n+1)=\prod_{k=1}^{n-1}(1-x_k)-\prod_{k=1}^{n}(1-x_k)=$
$(1-(1-x_n))\prod_{k=1}^{n-1}(1-x_k)=x_n\prod_{k=1}^{n-1}(1-x_k).$
Cette expression est encore valable pour $n=1$ puisque $\mathbb{P}(X=1)=\mathbb{P}(X=1|X\geq 1)=x_1$.

4. Soit X une variable aléatoire à valeur dans $\mathbb{N}^*$ à taux de panne constant : $\forall n\in\mathbb{N}^*,\ x_n=x\in]0,1[$.
Alors, $\forall n\in\mathbb{N}^*,\ p(X=n)=x(1-x)^{n-1}:X\sim\mathcal{G}(x)$.
Réciproquement, supposons que $X\sim\mathcal{G}(x)$ pour un certain $x\in]0,1[$. Fixons $n\in\mathbb{N}^*$
Alors $\mathbb{P}(X\geq n)=\sum_{k=n}^{+\infty}x(1-x)^{k-1}=x\cdot\dfrac{(1-x)^{n-1}}{1-(1-x)}=(1-x)^{n-1}.$
On en déduit $x_n=\dfrac{\mathbb{P}(X=n)}{\mathbb{P}(X\geq n)}=\dfrac{x(1-x)^{n-1}}{(1-x)^{n-1}}=x.$

XIII.9.26 Matrice aléatoire (1) ★★

[Enoncé]

1. $\det(A)=X_1X_2$.
Ainsi, $\mathbb{P}(\det(A)=0)=\mathbb{P}(X_1X_2=0)=\mathbb{P}(\{X_1=0\}\cup\{X_2=0\})\leq\mathbb{P}(X_1=0)+\mathbb{P}(X_2=0)=0$.
D'où $\mathbb{P}(\det(A)=0)=0$: A est presque sûrement inversible.

2. Soit $\omega\in\Omega$. Si $X_1(\omega)=X_2(\omega)=x$ alors $A(\omega)=\begin{pmatrix}x&1\\0&x\end{pmatrix}$ n'est pas diagonalisable puisque que son spectre ne contient que x et qu'elle est différente de $x\mathrm{I}_2$.
Et si $X_1(\omega)\neq X_2(\omega)$ alors $A(\omega)$ est diagonalisable puisque à spectre simple : $\mathrm{Sp}(A(\omega))=\{X_1(\omega),X_2(\omega)\}$.
Ainsi si l'on note D l'évènement "A est diagonalisable" on a,
$\mathbb{P}(\overline{D})=\mathbb{P}(X_1=X_2)=\sum_{n=1}^{+\infty}\mathbb{P}(X_1=n,X_2=n)=\sum_{n=1}^{+\infty}\mathbb{P}(X_1=n)\mathbb{P}(X_2=n)=$

$$p^2 \sum_{n=1}^{+\infty} \left((1-p)^2\right)^{n-1} = \frac{p^2}{1-(1-p)^2}$$

Et donc $\mathbb{P}(D) = 1 - \mathbb{P}(\overline{D}) = 1 - \dfrac{p^2}{p(2-p)} = \dfrac{2p(1-p)}{p(2-p)} = \dfrac{2(1-p)}{2-p}$.

XIII.9.27 Matrice aléatoire (2)

[Enoncé]

XIII.9.28 Matrice aléatoire (3)

[Enoncé]

XIII.9.29 Matrice aléatoire (4)

[Enoncé]

XIII.9.30 Matrice aléatoire (5)

[Enoncé]

XIII.9.31 Matrice aléatoire (6)

[Enoncé]

XIII.9.32 Matrice aléatoire (7)

[Enoncé]

XIII.9.33 Matrice de Rademacher

XIII.9.34 Vecteur propre aléatoire

XIII.9.35 Equation différentielle à coefficients aléatoires

[Enoncé]

XIII.9.36 Série entière aléatoire

[Enoncé]

XIII.9.37 Permutation aléatoire

[Enoncé]

XIII.9.38 Permutations composées d'un grand cycle

[Enoncé]

XIII.9.39 Loi conjointe (1) ★★

[Enoncé]

1. On doit avoir $\sum_{(n,k)\in\mathbb{N}^2} \mathbb{P}(X=k,Y=n)=1$.
   On applique le théorème de Fubini pour une famille positive,
   $$\sum_{(n,k)\in\mathbb{N}^2} \mathbb{P}(X=k,Y=n)=\sum_{n=0}^{+\infty}\sum_{k=0}^{+\infty}\mathbb{P}(X=k,Y=n)=\sum_{n=0}^{+\infty}a^n p(1-p)^n\sum_{k=0}^{n}\binom{n}{k}1^k\cdot 1^{n-k}=p\sum_{n=0}^{+\infty}(2a(1-p))^n=\frac{p}{1-2a(1-p)}.$$
   Donc $a=\dfrac{1}{2}$.
2. Soit $n\in\mathbb{N}$.
   D'après la formule des probabilités totales,
   $$\mathbb{P}(Y=n)=\sum_{k=0}^{+\infty}\mathbb{P}(X=k,Y=n)=p(1-p)^n\frac{1}{2^n}\sum_{k=0}^{n}\binom{n}{k}=p(1-p)^n.$$
   $Y+1\sim\mathcal{G}(p)$.
3. Soit $k\in\mathbb{N}$.
   D'après la formule des probabilités totales,
   $$\mathbb{P}(X=k)=\sum_{n=0}^{+\infty}\mathbb{P}(X=k,Y=n)=p\sum_{n=k}^{+\infty}\binom{n}{k}\left(\frac{1-p}{2}\right)^n=p\left(\frac{1-p}{2}\right)^k\sum_{n=k}^{+\infty}\binom{n}{k}\left(\frac{1-p}{2}\right)^{n-k}=\frac{p\left(\frac{1-p}{2}\right)^k}{\left(1-\frac{1-p}{2}\right)^{k+1}}.$$

C'est à dire, $\mathbb{P}(X=k)=\dfrac{2p}{1+p}\left(\dfrac{1-p}{1+p}\right)^k=\dfrac{2p}{1+p}\left(1-\dfrac{2p}{1+p}\right)^k$.

$X+1\sim\mathcal{G}\left(\dfrac{2p}{1+p}\right)$.

4. X et Y ne sont pas indépendantes. En effet, $\mathbb{P}(X=1,Y=0)=0\neq\mathbb{P}(X=1)\mathbb{P}(Y=0)$.

XIII.9.40 Loi conjointe (2) ★★★

[Enoncé]

1. On doit avoir $\displaystyle\sum_{0\leq i,j\leq n}\mathbb{P}(X=i,Y=j)=1$.

   Or, $\displaystyle\sum_{0\leq i,j\leq n}\mathbb{P}(X=i,Y=j)=\lambda\sum_{i=0}^{n}\binom{n}{i}\sum_{j=0}^{n}\binom{n}{j}=\lambda\left(\sum_{k=0}^{n}\binom{n}{k}1^k\cdot 1^{n-k}\right)^2=\lambda\left((1+1)^n\right)^2=\lambda 4^n$.

   Donc $\lambda=\dfrac{1}{4^n}$.

2. Soit $i\in[\![0;n]\!]$. D'après la formule des probabilités totales,

   $\mathbb{P}(X=i)=\displaystyle\sum_{j=0}^{n}\mathbb{P}(X=i,Y=j)=\frac{1}{4^n}\binom{n}{i}\sum_{j=0}^{n}\binom{n}{j}=\frac{1}{2^n}\binom{n}{i}$.

   Par symétrie, $\forall j\in[\![0;n]\!],\ \mathbb{P}(Y=j)=\dfrac{1}{2^n}\binom{n}{j}$.

3. $\forall(i,j)\in[\![0;n]\!]^2,\ \mathbb{P}(X=i,Y=j)=\mathbb{P}(X=i)\mathbb{P}(Y=j)\implies X\perp\!\!\!\perp Y$.

4. Notons $C=\left(\dfrac{1}{2^n}\binom{n}{j}\right)_{0\leq j\leq n}\in\mathcal{M}_{n,1}(\mathbb{R})$.

   $B=\left(\dfrac{1}{2^n}\binom{n}{0}C\ \middle|\ \dfrac{1}{2^n}\binom{n}{1}C\ \middle|\ \cdots\ \middle|\ \dfrac{1}{2^n}\binom{n}{i}C\ \middle|\ \cdots\ \middle|\ \dfrac{1}{2^n}\binom{n}{n-1}C\ \middle|\ \dfrac{1}{2^n}\binom{n}{n}C\right)=CC^\top$.

   Donc $\forall p\in\mathbb{N}^*,\ B^p=\left(CC^\top\right)^p=C\left(C^\top C\right)^{p-1}C^\top=\left(C^\top C\right)^{p-1}CC^\top=\left(C^\top C\right)^{p-1}B$. $\left(\left(C^\top C\right)^{p-1}\right.$ est un scalaire$\left.\right)$. Et on calcule $C^\top C=\mathrm{Tr}(C^\top C)=\mathrm{Tr}(CC^\top)=\mathrm{Tr}(B)=\dfrac{1}{4^n}\displaystyle\sum_{k=0}^{n}\binom{n}{k}^2=\frac{1}{4^n}\binom{2n}{n}$. *(la dernière égalité provient de l'identité de Vandermonde et n'est pas nécessaire)*

   Ainsi, $B^p=\mathrm{Tr}(B)^{p-1}B$.

5. $X^2-\mathrm{Tr}(B)X=X(X-\mathrm{Tr}(B))$ annule B et est scindé à racines simples donc B est diagonalisable et $\mathrm{Sp}(B)=\{0,\mathrm{Tr}(B)\}$.

$\mathrm{rg}(B) = 1$ donc on sait que $\dim(\mathrm{Ker}(B)) = n-1$ et $\dim(\mathrm{Ker}(B - \mathrm{Tr}(B)\mathrm{I}_n)) = 1$.
On remarque que $BC = C\left(C^\top C\right) = \mathrm{Tr}(B)C$ et que pour tout $j \in [\![2; n]\!]$, $BX_j = 0$ avec $X_j = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ -1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ où le coefficient -1 est en j-ième position.
Ainsi, $\mathrm{Ker}(B) = \mathrm{Vect}(C)$ et $\mathrm{Ker}(B - \mathrm{Tr}(B)I_n) = \mathrm{Vect}(X_2, \dots, X_n)$.

XIII.9.41 Fonction caractéristique ★★

[Enoncé]

1. Si $t \in \mathbb{R}$, la famille $\left(\mathbb{P}(X=k)e^{itk}\right)_{k\in\mathbb{Z}}$ est sommable puisque $\sum_{k\in\mathbb{Z}} \left|\mathbb{P}(X=k)e^{itk}\right| = \sum_{k\in\mathbb{Z}} \mathbb{P}(X=k) = 1 < +\infty$. Ainsi φ_X est définie sur $\mathbb{R}$. φ_X est clairement 2π-périodique.
   Notons pour $k \in \mathbb{Z}$, $f_k : t \in \mathbb{R} \mapsto \mathbb{P}(X=k)e^{itk}$
   Les série de fonctions $\sum_{k\in\mathbb{N}} f_k$ et $\sum_{k\in\mathbb{N}^*} f_{-k}$ convergent normalement, a fortiori uniformément, sur $\mathbb{R}$ puisque $\sum_{k\in\mathbb{N}} ||f_k||_\infty = \sum_{k\in\mathbb{N}} \mathbb{P}(X=k) \leq 1 < +\infty$ et $\sum_{k\in\mathbb{N}} ||f_{-k}||_\infty = \sum_{k\in\mathbb{N}^*} \mathbb{P}(X=-k) \leq 1 < +\infty$.
   Les fonctions f_k, $k \in \mathbb{Z}$ étant toutes continues sur $\mathbb{R}$, par transfert de continuité, $\varphi_X = \sum_{k\in\mathbb{N}} f_k + \sum_{k\in\mathbb{N}^*} f_{-k}$ est continue sur $\mathbb{R}$.
2. Pour tout $k \in \mathbb{Z}$ f_k est $\mathcal{C}^1$ sur $\mathbb{R}$ et, $\forall t \in \mathbb{R}$, $f_k'(t) = ik\mathbb{P}(X=k)e^{itk}$.
   Encore une fois les séries $\sum_{k\in\mathbb{N}} f_k'$ et $\sum_{k\in\mathbb{N}^*} f_{-k}'$ convergent normalement, a fortiori uniformément, sur $\mathbb{R}$ puisque $\sum_{k\in\mathbb{N}} ||f_k'||_\infty = \sum_{k\in\mathbb{N}} k\mathbb{P}(X=k) \leq \mathbb{E}(X) < +\infty$ et $\sum_{k\in\mathbb{N}} ||f_{-k}'||_\infty = \sum_{k\in\mathbb{N}^*} -k\mathbb{P}(X=-k) \leq \mathbb{E}(X) < +\infty$.
   Donc par théorème de transfert $\mathcal{C}^1$, φ_X est $\mathcal{C}^1$ sur $\mathbb{R}$ et,
   $\forall t \in \mathbb{R}$, $\varphi_X'(t) = \sum_{k\in\mathbb{N}} f_k'(t) + \sum_{k\in\mathbb{N}^*} f_{-k}'(t) = \sum_{k\in\mathbb{Z}} ik\mathbb{P}(X=k)e^{itk}$.

   On en déduit que $\mathbb{E}(X) = \dfrac{\varphi_X'(0)}{i} = -i\varphi_X'(0)$.

3. Pour tout $k \in \mathbb{Z}$ f_k est $\mathcal{C}^2$ sur $\mathbb{R}$ et, $\forall t \in \mathbb{R}$ $f_k''(t) = -k^2\mathbb{P}(X=k)e^{itk}$.
Encore une fois les séries $\sum_{k\in\mathbb{N}} f_k''$ et $\sum_{k\in\mathbb{N}^*} f_{-k}''$ convergent normalement, a fortiori uniformément, sur $\mathbb{R}$ puisque $\sum_{k\in\mathbb{N}} ||f_k''||_\infty = \sum_{k\in\mathbb{N}} k^2\mathbb{P}(X=k) \leq \mathbb{E}(X^2) < +\infty$ et $\sum_{k\in\mathbb{N}} ||f_{-k}''||_\infty = \sum_{k\in\mathbb{N}^*} (-k)^2\mathbb{P}(X=-k) \leq \mathbb{E}(X^2) < +\infty$.
Donc par théorème de transfert $\mathcal{C}^2$, φ_X est $\mathcal{C}^2$ sur $\mathbb{R}$ et,
$\forall t \in \mathbb{R},\ \varphi_X''(t) = \sum_{k\in\mathbb{N}} f_k''(t) + \sum_{k\in\mathbb{N}^*} f_{-k}''(t) = \sum_{k\in\mathbb{Z}} -k^2\mathbb{P}(X=k)e^{itk}$.

On en déduit que $\mathbb{V}(X) = \mathbb{E}(X^2) - \mathbb{E}(X)^2 = \sum_{k\in\mathbb{Z}} k^2\mathbb{P}(X=k) - \left(\frac{\varphi_X'(0)}{i}\right)^2 = \varphi_X'(0)^2 - \varphi_X''(0)$.

XIII.9.42 Fonction génératrice des moments ★★★★★

[Enoncé]

1. $\mathbb{E}(e^{0\cdot X}) = \mathbb{E}(1) = 1 < +\infty$. Donc $0 \in I_X$. Si $I_X = \{0\}$ alors c'est un intervalle. Supposons que I_X ne soit pas réduit à $\{0\}$.
Soient $a, b \in I_X$ tels que $a < b$ et soit $t \in [a,b]$.
$\forall \omega \in \Omega,\ X(\omega) \geq 0 \implies aX(\omega) \leq tX(\omega) \leq bX(\omega) \implies e^{tX(\omega)} \leq e^{bX(\omega)}$.
Et $\forall \omega \in \Omega,\ X(\omega) < 0 \implies aX(\omega) \geq tX(\omega) \geq bX(\omega) \implies e^{tX(\omega)} \leq e^{aX(\omega)}$.
Ainsi,

$$\begin{aligned}
\sum_{x\in X(\Omega)} e^{tx}\mathbb{P}(X=x) &= \sum_{x\in X(\Omega)\cap\mathbb{R}_-^*} e^{tx}\mathbb{P}(X=x) + \sum_{x\in X(\Omega)\cap\mathbb{R}_+^*} e^{tx}\mathbb{P}(X=x) \\
&\leq \sum_{x\in X(\Omega)\cap\mathbb{R}_-^*} e^{ax}\mathbb{P}(X=x) + \sum_{x\in X(\Omega)\cap\mathbb{R}_+^*} e^{bx}\mathbb{P}(X=x) \\
&\leq \sum_{x\in X(\Omega)} e^{ax}\mathbb{P}(X=x) + \sum_{x\in X(\Omega)} e^{bx}\mathbb{P}(X=x) \\
&= \mathbb{E}\left(e^{aX}\right) + \mathbb{E}\left(e^{bX}\right) \\
&< +\infty
\end{aligned}$$

Donc $e^{tX} \in L^1$ c'est à dire $t \in I_X$.
I_X est bien un intervalle.

2. Par hypothèse, $\exists a \in \mathbb{R}_+^*,\ ]-a,a[\subset I_X$.
On sait que $X(\Omega)$ est au plus dénombrable.
Si $X(\Omega) = \{x_0, \dots, x_p\}$ est fini alors il n'y a pas de difficulté,

$\forall t \in]-a,a[,\ M_X(t) = \sum_{k=0}^{p} e^{tx_k}\mathbb{P}(X=x_k) = \sum_{k=0}^{p}\sum_{n=0}^{+\infty}\frac{(tx)^n}{n!}\mathbb{P}(X=x_k) = \sum_{n=0}^{+\infty}\frac{t^n}{n!}\sum_{k=0}^{p}x_k^n\mathbb{P}(X=x_k) = \sum_{n=0}^{+\infty}\frac{\mathbb{E}(X^n)}{n!}t^n$

Supposons que $X(\Omega)$ est dénombrable. On note alors $X(\Omega) = \{x_n,\ n \in \mathbb{N}\}$. Montrons que M_X est $\mathcal{C}^\infty$ sur $]-a,a[$ et que $\forall p \in \mathbb{N},\ M_X^{(p)}(0) = \mathbb{E}(X^p)$.

Posons, pour $n \in \mathbb{N},\ f_n : t \in]-a,a[\mapsto \mathbb{P}(X=x_n)e^{tx_n}$.

Pour tout $n \in \mathbb{N},\ f_n$ est $\mathcal{C}^\infty$ sur $]-a,a[$ et $\forall t \in]-a,a[,\ \forall p \in \mathbb{N},\ f_n^{(p)}(t) = \mathbb{P}(X=x_n)x_n^p e^{tx_n}$.

Fixons maintenant $\alpha \in]0,a[$ et $\rho \in]\alpha,a[$.

On peut écrire $\forall n \in \mathbb{N},\ \forall t \in [-\alpha,\alpha],\ |f_n^{(p)}(t)| \leq |x_n^p|\mathbb{P}(X=x_n)e^{\alpha|x_n|}$.

Ensuite, on écrit $\forall n \in \mathbb{N},\ |x_n^p|\mathbb{P}(X=x_n)e^{\alpha|x_n|} = |x_n^p|e^{(\alpha-\rho)|x_n|} \times \mathbb{P}(X=x_n)e^{\rho|x_n|}$.

D'une part la fonction $u \mapsto u^p e^{(\alpha-a)u}$ est continue sur $\mathbb{R}_+$ et de limite nulle en $+\infty$, elle est donc bornée sur $\mathbb{R}_+$. On note alors $M_p \in \mathbb{R}_+$ tel que $\forall n \in \mathbb{N},\ |x_n|^p e^{(\alpha-a)|x_n|} \leq M_p$.

Donc, $\forall n \in \mathbb{N},\ \forall p \in \mathbb{N},\ ||f_n^{(p)}||_{\infty,[-\alpha,\alpha]} \leq M_p\mathbb{P}(X=x_n)e^{\rho|x_n|}$.

D'autre part, $\mathbb{P}(X=x_n)e^{\rho|x_n|} \leq \mathbb{P}(X=x_n)e^{\rho x_n} + \mathbb{P}(X=x_n)e^{-\rho x_n}$

Finalement, $\sum_{n=0}^{+\infty}||f_n||_{\infty,[-\alpha,\alpha]} \leq M_p\left(\sum_{n=0}^{+\infty}f_n(\rho) + \sum_{n=0}^{+\infty}f_n(-\rho)\right) < +\infty$ (car $(-\rho,\rho) \in I_X^2$).

On en déduit que $\sum_{n\in\mathbb{N}} f_n$ converge uniformément sur $[-\alpha,\alpha]$. Ceci étant vrai pour tout segment $[-\alpha,\alpha]$ de $]-a,a[$, $\sum_{n\in\mathbb{N}} f_n$ converge uniformément sur $]-a,a[$.

D'après le théorème de transfert $\mathcal{C}^\infty$, M_X est $\mathcal{C}^\infty$ sur $]-a,a[$ et $\forall p \in \mathbb{N},\ \forall t \in]-a,a[,\ M_X^{(p)}(t) = \sum_{n=0}^{+\infty}x_n^p\mathbb{P}(X=x_n)e^{tx_n}$.

Et par conséquent, $\forall p \in \mathbb{N},\ M_X^{(p)}(0) = \sum_{n=0}^{+\infty}x_n^p\mathbb{P}(X=x_n) = \mathbb{E}(X^p)$.

Soit $t \in]-a,a[$. $M_X(t) = \sum_{k=0}^{+\infty}\mathbb{P}(X=x_k)e^{tx_k} = \sum_{k=0}^{+\infty}\sum_{n=0}^{+\infty}\mathbb{P}(X=x_k)\frac{(tx_k)^n}{n!} = \sum_{k=0}^{+\infty}\sum_{n=0}^{+\infty}x_k^n\mathbb{P}(X=x_k)\frac{t^n}{n!}$.

Or la famille $\left(x_k^n\mathbb{P}(X=x_k)\frac{t^n}{n!}\right)_{(n,k)\in\mathbb{N}^2}$ est sommable. En effet, d'après le théorème de Fubini pour les familles positives,

$\sum_{k=0}^{+\infty}\sum_{n=0}^{+\infty}\left|x_k^n\mathbb{P}(X=x_k)\frac{t^n}{n!}\right| = \sum_{n=0}^{+\infty}\frac{|t|^n}{n!}\sum_{k=0}^{+\infty}|x_k|^n\mathbb{P}(X=x_k) = \sum_{n=0}^{+\infty}\frac{\mathbb{E}\left(|X|^n\right)}{n!}|t|^n$.

XIII.9.43 Inégalité de Jensen ★

[Enoncé]

1. $\mathbb{E}(X) \in \mathbb{R}$ donc comme f est dérivable et convexe sur $\mathbb{R}$,
   $\forall x \in \mathbb{R},\ f(x) \geq f'(\mathbb{E}(X))(x - \mathbb{E}(X)) + f(\mathbb{E}(X))$.
   $X(\Omega) \subset \mathbb{R}$ donc l'inégalité est vraie en termes de variables aléatoires :

$$f(X) \geq f'(\mathbb{E}(X))(X - \mathbb{E}(X)) + f(\mathbb{E}(X))$$

2. Supposons que $f(X) \in L^1$.
   Alors par croissance de l'espérance,

$$\begin{aligned}\mathbb{E}(f(X)) &\geq \mathbb{E}[f'(\mathbb{E}(X))(X - \mathbb{E}(X)) + f(\mathbb{E}(X))] \\ (f'(\mathbb{E}(X)) \text{ et } \mathbb{E}(X) \text{ sont des constantes}) &= f'(\mathbb{E}(X))(\mathbb{E}(X) - \mathbb{E}(X)) + \mathbb{E}(f(\mathbb{E}(X))) \\ (f(\mathbb{E}(X)) \text{ est une constante}) &= f(\mathbb{E}(X))\end{aligned}$$

XIII.9.44 Inégalité de Hölder ★★

[Enoncé]

1. L'inégalité est trivialement vérifiée si x ou y est nul. Soient $x, y \in \mathbb{R}_+^*$.
   La fonction ln est deux fois dérivable sur $\mathbb{R}_+^*$ et $\forall t > 0,\ \ln''(t) = -\dfrac{1}{t^2} \leq 0$. Donc ln est concave sur $\mathbb{R}_+^*$.
   Par conséquent d'après l'inégalité de Jensen $\forall u, v > 0,\ \dfrac{1}{p}\ln(u) + \dfrac{1}{q}\ln(v) \leq \ln\left(\dfrac{u}{p} + \dfrac{v}{p}\right)$.
   En appliquant cette inégalité pour $u = x^p$ et $v = y^q$ on obtient :

$$\ln(x) + \ln(y) \leq \ln\left(\frac{x^p}{p} + \frac{y^q}{q}\right)$$

   Puis en passant à l'exponentielle qui est une fonction strictement croissante :

$$xy \leq \frac{x^p}{p} + \frac{y^q}{q}$$

2. Supposons que $\mathbb{E}(X^p) = \mathbb{E}(Y^q) = 1$.
   Soit $\omega \in \Omega$. $X(\omega), Y(\omega) \in \mathbb{R}_+$ donc, $X(\omega)Y(\omega) \leq \dfrac{X(\omega)^p}{p} + \dfrac{Y(\omega)^q}{q}$ i.e $(XY)(\omega) \leq \dfrac{X^p(\omega)}{p} + \dfrac{Y^q(\omega)}{q}$. Alors en passant à l'espérance,

$$\mathbb{E}(XY) \leq \frac{\mathbb{E}(X^p)}{p} + \frac{\mathbb{E}(Y^q)}{q} = \frac{1}{p} + \frac{1}{q} = 1 = \mathbb{E}(X^p)^{1/p}\mathbb{E}(Y^q)^{1/q}$$

Revenons au cas général. Tout d'abord si $\mathbb{E}^p(X) = 0$ alors X^p est presque sûrement nulle puisque c'est une variable aléatoire positive. Donc X est presque sûrement nulle et par suite $\mathbb{E}(X) = 0$. De même, $\mathbb{E}(Y^q) = 0 \implies \mathbb{E}(Y) = 0$. L'inégalité est donc trivialement vérifiée dans ces cas.
On suppose maintenant $\mathbb{E}(X^p) \neq 0$ et $\mathbb{E}(Y^q) \neq 0$. On pose $X_0 = \dfrac{X}{\mathbb{E}(X^p)^{1/p}}$ et $Y_0 = \dfrac{Y}{\mathbb{E}(Y^q)^{1/q}}$. X_0 et Y_0 sont deux variables aléatoires réelles positives vérifiant $\mathbb{E}(X_0^p) = \mathbb{E}(Y_0^q) = 1$. D'après ce qui a été fait précédemment on sait que

$$\mathbb{E}(X_0 Y_0) \leq \mathbb{E}(X_0^p)^{1/p}\mathbb{E}(Y_0^q)^{1/q}$$

C'est à dire $\dfrac{\mathbb{E}(XY)}{\mathbb{E}(X^p)^{1/p}\mathbb{E}(Y^q)^{1/q}} \leq 1$ ou encore $\mathbb{E}(XY) \leq \mathbb{E}(X^p)^{1/p}\mathbb{E}(Y^q)^{1/q}$.

3. Pour $p = q = 2$ on a $\mathbb{E}(XY) \leq \sqrt{\mathbb{E}(X^2)\mathbb{E}(Y^2)}$. Il s'agit de l'inégalité de Cauchy-Schwartz.

XIII.9.45 Modes de convergences

[Enoncé]

XIII.9.46 Marche aléatoire sur $\mathbb{Z}^d$ ★★★

[Enoncé]

Le cas $d = 1$ ★★

1. Soit $t \in \mathbb{N}^*$. $Y_t(\Omega) = \{0, 1\} : Y_t \sim \mathcal{B}(\mathbb{P}(Y_t = 1)) = \mathcal{B}(\mathbb{P}(X_t = 1)) = \mathcal{B}(p)$.
Soit $n \in \mathbb{N}^*$.
$X_1, \dots, X_n$ sont mutuellement indépendantes donc d'après le lemme des coalitions, $Y_1, \dots, Y_n$ sont mutuellement indépendantes. Ainsi d'après le cours, $\displaystyle\sum_{t=1}^{n} Y_t \sim \mathcal{B}(n, p)$.

2. Soit $n \in \mathbb{N}^*$.
$S_n \displaystyle\sum_{t=1}^{n} X_t = \sum_{t=1}^{n}(2Y_t - 1) = 2\sum_{t=1}^{n} Y_t - n$.
Ainsi, si n est impair alors $S_n(\Omega) \subset \mathbb{Z}\backslash 2\mathbb{Z}$ et donc $\{S_n = 0\} = \emptyset$ d'où $\mathbb{P}(S_n = 0) = 0$.
Et si $n \in 2\mathbb{N}$ alors, $\mathbb{P}(S_n = 0) = \mathbb{P}\left(\displaystyle\sum_{t=1}^{n} Y_t = \frac{n}{2}\right) = \binom{n}{n/2}(p(1-p))^{n/2}$.

3. On utilise la formule de Stirling :

$$\mathbb{P}(S_{2n} = 0) = \frac{(2n)!}{(n!)^2}(p(1-p))^n \underset{n\to+\infty}{\sim} (p(1-p))^n \frac{\left(\frac{2n}{e}\right)^{2n}\sqrt{4\pi n}}{\left(\left(\frac{n}{e}\right)^n\sqrt{2\pi n}\right)^2} = \frac{(4p(1-p))^n}{\sqrt{\pi n}}.$$

Donc, $\lim\limits_{n\to+\infty} \mathbb{P}(S_{2n}=0) \in \{0,+\infty\}$ et,

$\lim\limits_{n\to+\infty} \mathbb{P}(S_{2n}=0) = +\infty \iff 4p(1-p) > 1 \iff p(1-p) > \dfrac{1}{4}$.

Or la fonction $x \in]0,1[\mapsto x(1-x)$ admet un maximum en $x = \dfrac{1}{2}$ qui vaut $\dfrac{1}{4}$.

Donc $\lim\limits_{n\to+\infty} \mathbb{P}(S_{2n}=0) = 0$.

On peut interpréter cela comme le fait que la puce ne retourne presque sûrement plus en l'origine après un certain temps.

4. $O_{2j}(\Omega) = \{0,1\}$ et $\{O_{2j}=1\} = \{S_{2j}=0\}$ donc $O_{2j} \sim \mathcal{B}(\mathbb{P}(S_{2j}=0)) = \mathcal{B}\left(\binom{2j}{j}(p(1-p))^j\right)$.

   Donc par linéarité de l'espérance, $\mathbb{E}(T_n) = \sum\limits_{j=0}^{n} \mathbb{E}(O_{2j}) = \sum\limits_{j=0}^{n} \binom{2j}{j}(p(1-p))^j$

5. Soit $x \in]-1,1[$.

   On sait que $\dfrac{1}{\sqrt{1-x}} = \sum\limits_{n=0}^{+\infty} \binom{-1/2}{n}(-x)^n$ avec,

   $$\binom{-1/2}{n} = \frac{1}{n!}\prod_{k=0}^{n-1}\left(-\frac{1}{2}-k\right) = \frac{(-1)^n}{2^n n!}\prod_{k=0}^{n-1}(2k+1) = \frac{(-1)^n}{2^n n!}\cdot\frac{\prod\limits_{k=1}^{2n} k}{\prod\limits_{k=1}^{n} 2k} = \frac{(-1)^n(2n)!}{2^{2n}(n!)^2} =$$

   $$\frac{(-1)^n}{4^n}\binom{2n}{n}.$$

   Donc $\dfrac{1}{\sqrt{1-x}} = \sum\limits_{n=0}^{+\infty} \binom{2n}{n}\left(\dfrac{x}{4}\right)^n$.

   $p \neq \dfrac{1}{2} \implies 0 < 4p(1-p) < 1$ donc,

   $\lim\limits_{n\to+\infty} \mathbb{E}(T_n) = \sum\limits_{n=0}^{+\infty} \binom{2n}{n}\left(\dfrac{4p(1-p)}{4}\right)^n = \dfrac{1}{\sqrt{1-4p(1-p)}}$.

   On peut interpréter qu'en moyenne, la puce est repassée $\dfrac{1}{\sqrt{1-4p(1-p)}}$ fois par l'origine lors de son parcours.

6. Soit $n \in \mathbb{N}$.

   $\mathbb{E}(T_n) = \sum\limits_{j=0}^{n} \binom{2j}{j}\dfrac{1}{4^n}$ donc $\mathbb{E}(T_0) = 0 = \dfrac{2\times 0+1}{2^{2\times 0}}\binom{0}{0}$.

   Supposons que $\mathbb{E}(T_n) = \dfrac{2n+1}{2^{2n}}\binom{2n}{n}$.

   Alors, $\mathbb{E}(T_{n+1}) = \mathbb{E}(T_n) + \mathbb{P}(S_{2n+2}=0) = \dfrac{2n+1}{4^n}\binom{2n}{n} + \binom{2n+2}{n+1}\dfrac{1}{4^{n+1}}$

Et $\binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \frac{(n+1)^2}{(2n+1)(2n+2)} \cdot \frac{(2n+2)!}{((n+1)!)^2} = \frac{2(n+1)}{4(2n+1)}\binom{2n+2}{n+1}$.

Donc, $\mathbb{E}(T_{n+1}) = \frac{1}{4^{n+1}}\binom{2n+2}{n+1}(2n+2+1) = \frac{2(n+1)+1}{4^{n+1}}\binom{2(n+1)}{n+1}$.

Ainsi par récurrence, $\forall n \in \mathbb{N},\ \mathbb{E}(T_n) = \frac{2n+1}{4^n}\binom{2n}{n}$.

On en déduit que $\mathbb{E}(T_n) \underset{n\to+\infty}{\sim} \frac{2n+1}{\sqrt{\pi n}} \underset{n\to+\infty}{\sim} 2\sqrt{\frac{n}{\pi}}$ d'où $\mathbb{E}(T_n) \underset{n\to+\infty}{\longrightarrow} +\infty$.

La puce repasse, en moyenne, une infinité de fois par l'origine lors de son parcours. Ceci paraît cohérent pour une puce qui a autant de chance de se déplacer à gauche qu'à droite. Remarque : On aurait aussi pu utiliser l'équivalent $\mathbb{P}(S_{2n} = 0) \underset{n\to+\infty}{\sim} \frac{(4p(1-p))^n}{\sqrt{\pi n}} = \frac{1}{\sqrt{\pi n}} = \frac{2}{\sqrt{\pi}}\left(\sqrt{n+1} - \sqrt{n}\right)$ pour avoir l'équivalent, et donc la limite, de $(\mathbb{E}(T_n))_{n\in\mathbb{N}}$.

Le cas $d = 2$

Le cas général

Marche aléatoire auto-évitante

XIII.9.47 Matrice de covariance ★★

[Enoncé]

1. $A^\top X = \sum_{k=1}^{n} a_k X_k$.
   L^2 est un espace vectoriel donc $A^\top X \in L^2$ et par bilinéarité de la covariance,

$$\begin{aligned}\mathbb{V}(A^\top X) &= \mathrm{Cov}(A^\top X, A^\top X)\\ &= \mathrm{Cov}\left(\sum_{i=1}^{n} a_i X_i, \sum_{j=1}^{n} a_j X_j\right)\\ &= \sum_{1\le i,j\le n} a_i a_j \,\mathrm{Cov}(X_i, X_j)\\ &= A^\top \Sigma A\end{aligned}$$

2. La covariance étant symétrique, Σ est symétrique réelle et donc diagonalisable d'après le théorème spectral. De plus, la question précédente montre que $\forall A \in \mathcal{M}_{n,1}(\mathbb{R}),\ A^\top \Sigma A \ge 0$.
   Donc $\Sigma \in S_n^{++}(\mathbb{R})$ c'est à dire $\mathrm{Sp}(\Sigma) \subset \mathbb{R}_+$.

3. $0 \notin \mathrm{Sp}(\Sigma) \iff \forall A = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in \mathcal{M}_{n,1}(\mathbb{R}),\ A^\top \Sigma A = \mathbb{V}(A^\top X) \neq 0.$

   Or, pour toute variable aléatoire discrète réelle Y, $\mathbb{V}(Y) = 0 \iff \mathbb{E}((Y - \mathbb{E}(Y)^2) = 0$. Et puisque la variable aléatoire $(Y - \mathbb{E}(Y))^2$ est positive, cela équivaut à ce que $(Y - \mathbb{E}(Y))^2 = 0$ c'est à dire à ce que $Y = \mathbb{E}(Y)$ et donc à ce que Y soit certaine (constante).
   On peut alors donner la condition : Σ est inversible si et seulement s'il n'existe aucune combinaison linéaire de $X_1, \dots, X_n$ qui soit presque sûrement constante.
   Ou encore qu'il n'existe aucune combinaison affine de $X_1, \dots, X_n$ qui soit presque sûrement nulle.
   Remarque : On pourra apprécier la ressemblance, dans une certaine mesure, entre cette condition et celle pour la matrice de Gram.

XIII.9.48 Maximisation de la variance sous-contrainte

[Enoncé]

1. On note X_i la variable aléatoire qui vaut 1 si la i-ème ampoule est allumée.
   On a donc $X_i \sim \mathcal{B}(p_i)$.
   On a donc $Y = \sum_{i=1}^{n} X_i$.
   Par linéarité de l'espérance,

$$\mathbb{E}(Y) = \sum_{i=1}^{n} \mathbb{E}(X_i) = \sum_{i=1}^{n} p_i$$

   . Puisque les (X_i) sont indépendants par hypothèse, on a :

$$\mathbb{V}(Y) = \sum_{i=1}^{n} \mathbb{V}(X_i) = \sum_{i=1}^{n} p_i(1 - p_i)$$

2. On peut voir ce problème comme un problème d'optimisation sous contrainte.
   On pose $p = (p_1, \dots, p_n)$.
   On pose également $f(p) = \sum_{i=1}^{n} p_i(1 - p_i)$ et $g(p) = \sum_{i=1}^{n} p_i - m$.
   On a donc :

$$\begin{cases} \nabla f(p) = (1 - 2p_1, \dots, 1 - 2p_n) \\ \nabla g(p) = (1, \dots, 1) \end{cases}$$

   Cherchons $\lambda \in \mathbb{R}$ tel que $\nabla f(p) = \lambda \nabla g(p)$ quand $g(p) = 0$. Donc qu'un tel λ existe il faut que les p_i soient égaux, on a donc :

$$p_i = \frac{m}{n}$$

pour tout $i \in [\![1;n]\!]$. Ainsi, la variance est maximale pour $p = \left(\frac{m}{n}, \dots, \frac{m}{n}\right)$ et :

$$\mathbb{V}(Y) = \sum_{i=1}^{n} \frac{m}{n}\left(1 - \frac{m}{n}\right) = m(1 - \frac{m}{n})$$

On en déduit que : $Y \sim \mathcal{B}\left(n, \frac{m}{n}\right)$.

XIII.9.49 Inégalité de Kosmanek ★

[Enoncé]

1. $\mathbb{1}_C \sim \mathcal{B}(\mathbb{P}(C))$ donc $\mathbb{V}(\mathbb{1}_C) = \mathbb{P}(C)(1 - \mathbb{P}(C))$.
   Or la fonction $p \mapsto p(1-p)$ admet un maximum sur $[0,1]$ en $p = \frac{1}{2}$ qui vaut $\frac{1}{4}$.
   On en déduit que $\mathbb{V}(\mathbb{1}_C) \leq \frac{1}{4}$.
2. D'après l'inégalité de Cauchy-Schwartz, $|\mathrm{Cov}(\mathbb{1}_A, \mathbb{1}_B)| \leq \sqrt{\mathbb{V}(\mathbb{1}_A)\mathbb{V}(\mathbb{1}_B)} \leq \frac{1}{4}$.
3. $\frac{1}{4} \geq |\mathrm{Cov}(\mathbb{1}_A, \mathbb{1}_B)| = |\mathbb{E}(\mathbb{1}_A\mathbb{1}_B) - \mathbb{E}(\mathbb{1}_A)\mathbb{E}(\mathbb{1}_B)| = |\mathbb{E}(\mathbb{1}_{A\cap B}) - \mathbb{E}(\mathbb{1}_A)\mathbb{E}(\mathbb{1}_B)| = |\mathbb{P}(A \cap B) - \mathbb{P}(A)\mathbb{P}(B)|$.
   Il y a égalité lorsque $|\mathrm{Cov}(\mathbb{1}_A, \mathbb{1}_B)| = \sqrt{\mathbb{V}(\mathbb{1}_A)\mathbb{V}(\mathbb{1}_B)} = \frac{1}{4}$.
   La deuxième égalité impose $\mathbb{P}(A) = \mathbb{P}(B) = \frac{1}{2}$.
   Alors la première égalité devient $\left|\mathbb{P}(A \cap B) - \frac{1}{4}\right| = \frac{1}{4}$ c'est à dire $\mathbb{P}(A \cap B) = \frac{1}{2}$ ou $\mathbb{P}(A \cap B) = 0$.

XIII.9.50 Inégalité de Cantelli ★★★

[Enoncé]

1. (a) Soit $u \in \mathbb{R}_+$.
   $\mathbb{E}\left((X+u)^2\right) = \mathbb{E}(X^2 + 2uX + u^2) = \mathbb{E}(X^2) + 2u\mathbb{E}(X) + \mathbb{E}(u^2) = \mathbb{E}(X^2) - \mathbb{E}(X)^2 + u^2 = \mathbb{V}(X) + u^2$.
   (b) Soit $u \in \mathbb{R}_+$.
   $\mathbb{P}(X \geq \lambda) \leq \mathbb{P}(X + u \geq \lambda + u)$. Or $\lambda + u \geq 0$ donc, $\mathbb{P}(|X+u| \geq \lambda + u) = \mathbb{P}\left((X+u)^2 \geq (\lambda+u)^2\right)$.
   Enfin, $\{X + u \geq \lambda + u\} \subset \{|X+u| \geq \lambda + u\}$.
   Donc d'après l'inégalité de Markov, $\mathbb{P}(X \geq \lambda) \leq \mathbb{P}\left((X+u)^2 \geq (\lambda+u)^2\right) \leq \frac{\mathbb{E}\left((X+u)^2\right)}{(\lambda+u)^2} = \frac{\mathbb{V}(X) + u^2}{(\lambda+u)^2}$.

(c) Posons $f : \left\{ \begin{array}{ccc} \mathbb{R}_+ & \longrightarrow & \mathbb{R} \\ u & \longmapsto & \dfrac{\mathbb{V}(X)+u^2}{(\lambda+u)^2} \end{array} \right.$. f est dérivable sur $\mathbb{R}_+$ et pour tout $u \in \mathbb{R}_+$,

$$\begin{aligned} f'(u) &= \frac{2u(\lambda+u)^2 - 2(\mathbb{V}(X)+u^2)(\lambda+u)}{(\lambda+u)^4} \\ &= \frac{2(u\lambda^2 + 2\lambda u^2 + u^3 - \lambda\mathbb{V}(X) - \mathbb{V}(X)u - \lambda u^2 - u^3)}{(\lambda+u)^4} \\ &= \frac{2(\lambda u^2 + (\lambda^2 - \mathbb{V}(X))u - \lambda\mathbb{V}(X))}{(\lambda+u)^4} \end{aligned}$$

Ainsi, $\forall u \in \mathbb{R}_+,\ f'(u) \geq 0 \iff \lambda u^2 + (\lambda^2 - \mathbb{V}(X))u - \lambda\mathbb{V}(X) \geq 0$.

$\Delta = (\lambda^2 - \mathbb{V}(X))^2 + 4\lambda^2\mathbb{V}(X) = (\lambda^2 + \mathbb{V}(X))^2 > 0$. On pose $u_1 = \dfrac{\mathbb{V}(X) - \lambda^2 + \sqrt{\Delta}}{2\lambda} = \dfrac{\mathbb{V}(X)}{\lambda}$ et $u_2 = \dfrac{\mathbb{V}(X) - \lambda^2 - \sqrt{\Delta}}{2\lambda} = -\lambda < 0$.

En résumé,

x	0		u_1		$+\infty$
$f'(x)$		$-$	0	$+$	
Variations de f		↘	$f(u_1)$	↗	

Ainsi, l'inégalité optimale que l'on peut atteindre est donnée par $u = u_1$:

$$\mathbb{P}(X \geq \lambda) \leq \frac{\mathbb{V}(X) + \left(\dfrac{\mathbb{V}(X)}{\lambda}\right)^2}{\left(\lambda + \dfrac{\mathbb{V}(X)}{\lambda}\right)^2} = \frac{\lambda^2\mathbb{V}(X) + \mathbb{V}(X)^2}{(\lambda^2 + \mathbb{V}(X))^2} = \frac{\mathbb{V}(X)(\lambda^2 + \mathbb{V}(X))}{(\lambda^2 + \mathbb{V}(X))^2} = \frac{\mathbb{V}(X)}{\lambda^2 + \mathbb{V}(X)}.$$

2. La variable aléatoire $Y = X - \mathbb{E}(X)$ est réelle discrète et centrée ($\mathbb{E}(Y) = 0$). Elle possède un moment d'ordre 2 puisque d'après le cours, $\mathbb{V}(Y) = \mathbb{V}(X)$.
Par conséquent d'après ce qui a été fait précédemment,

$$\mathbb{P}(X - \mathbb{E}(X) \geq \lambda) = \mathbb{P}(Y \geq \lambda) \leq \frac{\mathbb{V}(Y)}{\lambda^2 + \mathbb{V}(Y)} = \frac{\mathbb{V}(X)}{\lambda^2 + \mathbb{V}(X)}$$

XIII.9.51 Inégalité de Hoeffding ★★★

[Enoncé]

1. Soient $t \in \mathbb{R}$ et $x \in [-1,1]$. On sait que la fonction exp est convexe sur $\mathbb{R}$ et on remarque que $\frac{1}{2}(1-x)+\frac{1}{2}(1+x)=1$ et que $\frac{1}{2}(1-x)(-t)+\frac{1}{2}(1+x)t = tx$.
   Donc $e^{tx} \leq \frac{1}{2}(1-x)e^{-t}+\frac{1}{2}(1+x)e^{t}$.

2. Soit $t \in \mathbb{R}$.
   On sait que $\mathrm{ch}(t) = \sum_{n=0}^{+\infty} \frac{t^{2n}}{(2n!)}$ et $e^{t^2/2} = \sum_{n=0}^{+\infty} \frac{\left(\frac{t^2}{2}\right)^n}{n!} = \sum_{n=0}^{+\infty} \frac{t^{2n}}{2^n n!}$.
   Or, $\forall n \in \mathbb{N}^*,\ \frac{(2n)!}{2^n n!} \geq \frac{(2n)!}{(n!)^2} = \binom{2n}{n} \geq 1$. Donc $\forall n \in \mathbb{N}^*,\ (2n)! \geq 2^n n!$.
   Ainsi, $\mathrm{ch}(t) - e^{t^2/2} = \sum_{n=1}^{+\infty} \left(\frac{1}{(2n)!} - \frac{1}{2^n n!}\right) t^{2n} \leq 0$.

3. Soit $t \in \mathbb{R}$. $\forall \omega \in \Omega,\ X(\omega) \in [-1,1]$. Donc d'après la question 1 et par croissance de l'espérance,
   $\mathbb{E}(e^{tX}) \leq \mathbb{E}\left(\frac{e^{-t}}{2}(1-X)+\frac{e^{t}}{2}(1+X)\right) = \frac{e^{-t}+e^{t}}{2} - \frac{1}{2}\mathbb{E}(X) + \frac{1}{2}\mathbb{E}(X) = \mathrm{ch}(t) \leq e^{t^2/2}$.

4. Soit $(t,\varepsilon) \in \left(\mathbb{R}_+^*\right)^2$. La variable aléatoire discrète e^{tY} est réelle et positive donc d'après l'inégalité de Markov,
   $\mathbb{P}(Y \geq \varepsilon) = \mathbb{P}(tY \geq t\varepsilon) = \mathbb{P}\left(e^{tY} \geq e^{t\varepsilon}\right) \leq e^{-t\varepsilon}\mathbb{E}\left(e^{tY}\right)$.

5. Soit $\varepsilon \in \mathbb{R}_+^*$. Notons $a = \sqrt{\sum_{k=1}^{n} c_k^2}$.
   $\frac{S}{a}$ et $-\frac{S}{a}$ sont des variables aléatoires discrètes centrées à valeurs dans $[-1,1]$ donc $\forall t \in \mathbb{R}_+^*$,

$$\begin{aligned}
\mathbb{P}(|S| \geq \varepsilon) &= \mathbb{P}(S \geq \varepsilon) + \mathbb{P}(-S \geq \varepsilon) \\
&= \mathbb{P}\left(\frac{S}{a} \geq \frac{\varepsilon}{a}\right) + \mathbb{P}\left(-\frac{S}{a} \geq \frac{\varepsilon}{a}\right) \\
&\leq e^{-t\varepsilon/a}\mathbb{E}\left(e^{tS/a}\right) + e^{-t\varepsilon/a}\mathbb{E}\left(e^{-tS/a}\right) \\
&\leq e^{-t\varepsilon/a}\left(e^{t^2/2} + e^{(-t)^2/2}\right) \\
&= 2e^{-t\varepsilon/a + t^2/2}
\end{aligned}$$

En particulier pour $t = \dfrac{\varepsilon}{a}$:

$$\mathbb{P}(|S| \geq \varepsilon) \leq 2\exp\left(-\frac{\varepsilon^2}{2a^2}\right) = 2\exp\left(-\frac{\varepsilon^2}{2\sum_{k=1}^{n} c_k^2}\right)$$

XIII.9.52 Théorème d'approximation de Weierstrass ★★★

[Enoncé]

1. D'après le cours, $S_n \sim \mathcal{B}(n,t)$ et donc, $\forall k \in [\![0;n]\!]$, $\mathbb{P}(S_n = k) = b_k^n(t)$. Posons $R_n = \dfrac{S_n}{n}$.
   R_n est une variable aléatoire comme somme de variables aléatoires. De plus $R_n(\Omega) = \left\{\dfrac{k}{n},\ k \in [\![0;n]\!]\right\}$ est fini. Ainsi, R_n est une variable aléatoire discrète et d'après la formule de transfert,
   $$\mathbb{E}(f(R_n)) = \sum_{k=0}^{n} f\left(\frac{k}{n}\right)\mathbb{P}\left(R_n = \frac{k}{n}\right) = \sum_{k=0}^{n} f\left(\frac{k}{n}\right)\mathbb{P}(S_n = k) = B_n(f)(t).$$
2. f est continue sur le segment I donc d'après le théorème de Heine, f est uniformément continue sur I.
   Par conséquent, $\exists \delta > 0,\ \forall (x,y) \in \mathbb{R}^2,\ |x-y| \leq \delta \implies |f(x) - f(y)| \leq \dfrac{\varepsilon}{2}$
   Comme $\{|t - R_n| \leq \delta\} \sqcup \{|t - R_n| > \delta\} = \Omega$, on peut écrire
   $|f(t) - f(R_n)| = |f(t) - f(R_n)|\mathbb{1}_{\{|t-R_n|\leq\delta\}} + |f(t) - f(R_n)|\mathbb{1}_{\{|t-R_n|>\delta\}}$.

   Or, $|f(t)-f(R_n)|\mathbb{1}_{\{|t-R_n|\leq\delta\}} \leq \dfrac{\varepsilon}{2}\mathbb{1}_{\{|t-R_n|\leq\delta\}}$ et $|f(t)-f(R_n)|\mathbb{1}_{\{|t-R_n|>\delta\}} \leq 2||f||_\infty \mathbb{1}_{\{|t-R_n|>\delta\}}$.
   Aussi on rappelle que pour tout évènement A, $\mathbb{E}(\mathbb{1}_A) = \mathbb{P}(A)$.
   Ainsi par croissance de l'espérance,

   $$\begin{aligned}\mathbb{E}(|f(t) - f(R_n)|) &= \mathbb{E}\left(|f(t) - f(R_n)|\mathbb{1}_{\{|t-R_n|\leq\delta\}}\right) + \mathbb{E}\left(|f(t) - f(R_n)|\mathbb{1}_{\{|t-R_n|>\delta\}}\right)\\ &\leq \frac{\varepsilon}{2}\mathbb{E}\left(\mathbb{1}_{\{|t-R_n|\leq\delta\}}\right) + 2||f||_\infty\mathbb{E}\left(\mathbb{1}_{\{|t-R_n|>\delta\}}\right)\\ &\leq \frac{\varepsilon}{2} + 2||f||_\infty\mathbb{P}\left(|t - R_n| > \delta\right)\end{aligned}$$

3. D'après l'inégalité de Cauchy-Schwartz,
   $\mathbb{P}(|R_n - t| > \delta) = \mathbb{P}(|R_n - \mathbb{E}(R_n)| > \delta) \leq \dfrac{\mathbb{V}(R_n)}{\delta^2} = \dfrac{\mathbb{V}(S_n)}{n^2\delta^2} = \dfrac{t(1-t)}{n\delta^2}$.

   Etudions $g : x \mapsto x(1-x)$ sur I. g est dérivable sur I et $\forall x \in I,\ g'(x) = 1 - 2x$.

x	0		$\frac{1}{2}$		1
$g'(x)$		$+$	0	$-$	
Variations de g	0	↗	$\frac{1}{4}$	↘	0

On en déduit la majoration $\mathbb{P}(|R_n - t| > \delta) \leq \dfrac{1}{4n\delta^2}$.

4. Soit $\varepsilon > 0$. Fixons $n \in \mathbb{N}^*$.
$|f(t) - B_n(f)(t)| = |f(t) - \mathbb{E}(R_n)| = |\mathbb{E}(f(t) - R_n)|$.
Or, $f(t) - R_n \leq |f(t) - R_n|$ et $R_n - f(t) \leq |f(t) - R_n|$ donc par croissance de l'espérance, $|\mathbb{E}(f(t) - R_n)| = \max(\mathbb{E}(f(t) - R_n), \mathbb{E}(R_n - f(t))) \leq \mathbb{E}(|f(t) - R_n|)$.
Ainsi d'après les questions 2 et 3,
$|f(t) - B_n(f)(t)| \leq \dfrac{\varepsilon}{2} + \dfrac{||f||_\infty}{2n\delta^2}$.
Et donc, $\forall n \geq N = \left\lfloor \dfrac{||f||_\infty}{\varepsilon\delta^2} \right\rfloor$, $|f(t) - B_n(f)(t)| \leq \varepsilon$
d'où, $\forall n \geq N$, $||f - B_n(f)||_\infty \leq \varepsilon$.

5. Soit $[a, b] \subset \mathbb{R}$. Soit $f \in \mathcal{C}^0([a, b], \mathbb{C})$.
Posons $\gamma : \begin{cases} [a,b] & \longrightarrow & I \\ t & \longmapsto & \dfrac{t-a}{b-a} \end{cases}$.
γ est continue et bijective donc $f \circ \gamma^{-1} \in \mathcal{C}$ et on pose alors, pour tout $n \in \mathbb{N}^*$, $A_n = B_n(f \circ \gamma^{-1}) \circ \gamma$.
$(A_n)_{n \in \mathbb{N}^*}$ est une suite de fonctions de $[a, b]$ dans $\mathbb{C}$ polynomiales.
Fixons $\varepsilon > 0$.
D'après la question 4, $\exists N \in \mathbb{N}^*$, $\forall n \geq N$, $\forall t \in [0, 1]$, $|f \circ \gamma^{-1}(t) - B_n(f \circ \gamma^{-1})(t)| \leq \varepsilon$.
C'est à dire, $\exists N \in \mathbb{N}^*$, $\forall n \geq N$, $\forall t \in [a, b]$, $|f(t) - A_n(t)| \leq \varepsilon$.
Ainsi, $||f - A_n||_{\infty,[a,b]} \underset{n \to +\infty}{\longrightarrow} 0$ ce qui termine la preuve.

XIII.10 Correction Endomorphismes d'un espace euclidien

XIII.10.1 Equations matricielles ★

[Enoncé]

1. Supposons qu'il existe A et B deux telles matrices.
   Alors $n = \mathrm{Tr}(I_n) = \mathrm{Tr}(AB - BA) = \mathrm{Tr}(AB) - \mathrm{Tr}(BA) = \mathrm{Tr}(AB) - \mathrm{Tr}(AB) = 0$ ce qui est absurde.
2. Supposons qu'il existe une telle matrice M.
   Alors $\det(M^2) = \det(M)^2 = \det\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = -1$.
   Or M est à coefficients réels donc $\det(M) \in \mathbb{R}$ ce qui est absurde.
3. Supposons qu'il existe une telle matrice N.
   Alors $N^4 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ et donc N est nilpotente. On en déduit que $\chi_N = X^2$. Mais alors d'après le théorème de Cayley-Hamilton, $N^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ ce qui est absurde.

XIII.10.2 Equation matricielle faisant intervenir la comatrice

[Enoncé]
Soit $A \in \mathcal{M}_n(R)$ telle que $Com(A) = A$.
On rappelle que

$$A\,\mathrm{Com}(A)^\top = \det(A) I_n$$

Ainsi, on en déduit que : $AA^\top = \det(A) I_n$.
Par passage au déterminant, $\det(A)^2 = \det(A)$.Donc $\det(A) = 0$ ou $\det(A) = 1$.
• Si $\det(A) = 0$ alors $AA^\top = 0$. Ainsi, $\mathrm{Tr}(A^\top A) = 0$ ce qui implique que : $A = 0$.
• Si $\det(A) = 1$ alors $AA^\top = I_n$ donc $A \in \mathcal{O}_n(\mathbb{R})$.
Réciproquement, il est clairement que si $A = 0$ alors $\mathrm{Com}(A) = A$.
Si $A \in \mathcal{SO}_n(\mathbb{R})$ alors $A^{-1} = A^\top$ et $\det(A) = 1$.
Donc puisque

$$A\,\mathrm{Com}(A)^\top = I_n$$

Donc par unicité de l'inverse $\mathrm{Com}(A)^\top = A^\top$. D'où $A = \mathrm{Com}(A)$.
Donc l'ensemble des solutions des matrices vérifiant $A = \mathrm{Com}(A)$ est :

$$\mathcal{SO}_n(\mathbb{R}) \cup \{0\}$$

XIII.10.3 Matrice de rotation

[Enoncé]
On pose $M = \mathrm{Mat}_{\mathcal{B}}(u)$.

$$M^\top M = \frac{1}{9}\begin{pmatrix} 2 & -2 & 1 \\ -2 & 1 & 2 \\ 1 & -2 & 2 \end{pmatrix}\begin{pmatrix} 2 & 2 & 1 \\ -2 & 1 & 2 \\ 1 & -2 & 2 \end{pmatrix} = \frac{1}{9}\begin{pmatrix} 9 & 0 & 0 \\ 0 & 9 & 0 \\ 0 & 0 & 9 \end{pmatrix} = I_n$$

Donc $u \in O(E)$. Calculons son déterminant à l'aide de la formule de Sarrus :

$$\det(M) = \frac{1}{27}(4+4+4-1+8+8) = 1$$

Donc u est une rotation.
Solution à la question bonus :
Pour déterminer l'axe, il suffit de trouver un vecteur x tel que $Mx = x$. On cherche donc à résoudre le système suivant :

$$\begin{cases} 2x + 2y + z = 3x \\ -2x + y + 2z = 3y \\ x - 2y + 2z = 3z \end{cases}$$

Après résolution, on obtient que $\mathrm{Vect}\left(\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}\right)$ est l'axe de rotation de u.
Trouvons maintenant son angle θ.
On sait que :

$$\mathrm{Tr}(M) = 1 + 2\cos(\theta) = 5$$

Donc $\cos(\theta) = \frac{\frac{5}{3}-1}{2} = \frac{1}{3}$
Donc $\theta = \pm \arccos\left(\frac{1}{3}\right)$.
Pour trouver le signe de l'angle, il suffit de regarder le signe le déterminant de la famille $\left(\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, x, Mx\right)$ avec x un vecteur non colinéaire à $\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$ On prenant $x = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$, on obtient que $\det(\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, x, Mx) < 0$.
Par conséquent, on a : $\theta < 0$ i.e $\theta = -\arccos\left(\frac{1}{3}\right)$.

XIII.10.4 Produit mixte et produit vectoriel

[Enoncé]

XIII.10.5 Hyperplan de $\mathcal{M}_n(\mathbb{K})$

[Enoncé]
Soit H un hyperplan de $\mathcal{M}_n(\mathbb{K})$.
Supposons que H ne contient aucun matrice inversible.
Ainsi puisque I_n est inversible, on a

$$H \bigoplus \text{Vect } I_n = \mathcal{M}_n(\mathbb{K})$$

Montrons que H contient toutes les matrices nilpotentes.
Soit N une matrice nilpotente.
D'après ce qui précède, il existe $A \in H$ et $\lambda \in \mathbb{K}$ tel que

$$N = A + \lambda I_n$$

Puisque $A \in H$, en particulier elle n'est pas inversible donc il existe $X \in \mathcal{M}_n(\mathbb{K})$ non nulle tel que $AX = 0$.
Cela implique que

$$NX = \lambda X$$

Donc X est un vecteur propre de N, on a a fortiori $\lambda = 0$, d'où $N = A \in H$.
En particulier H contient toutes les matrices $E_{i,j}$ pour $i \neq j$.
Donc la matrice J défini par

$$J = \begin{pmatrix} 0 & 1 & \dots & (0) \\ & \ddots & \ddots & \\ & (0) & \ddots & 1 \\ 1 & & & 0 \end{pmatrix}$$

est dans H.
Or cette matrice est inversible donc on a montré par l'absurde que toute hyperplan de $\mathcal{M}_n(\mathbb{K})$ rencontre $\text{GL}_n(\mathbb{K})$.

XIII.10.6 Equation entre projecteurs

[Enoncé]

XIII.10.7 Exemple de symétrie orthogonale

[Enoncé]
D'après le cours, il est évident que s est un symétrie.
Montrons qu'elle est orthogonale.
On remarque que $\text{Ker}(s - Id) = \mathcal{S}_n(\mathbb{R})$ et que $\text{Ker}(s + Id) = \mathcal{A}_n(\mathbb{R})$.

Il suffit de montrer que $\mathcal{S}_n(\mathbb{R})$ et $\mathcal{A}_n(\mathbb{R})$ sont orthogonaux. Soit $S \in \mathcal{S}_n(\mathbb{R})$ et $A \in \mathcal{A}_n(\mathbb{R})$.

$$\begin{cases} \operatorname{Tr}(A^\top S) = -\operatorname{Tr}(AS) \\ \operatorname{Tr}(S^\top A) = \operatorname{Tr}(SA) = \operatorname{Tr}(AS) \end{cases}$$

Donc, par symétrie du produit scalaire, on en déduit que $\langle A, S\rangle = 0$. Donc $\mathcal{S}_n(\mathbb{R})$ et $\mathcal{A}_n(\mathbb{R})$ sont orthogonaux.
Ainsi s est une symétrie orthogonale.

XIII.10.8 Caractérisations des projecteurs orthogonales

[Enoncé]

XIII.10.9 Norme d'une base orthogonale

[Enoncé]

XIII.10.10 Matrice de Hilbert

[Enoncé]

1. — *Symétrie* :
Soit $(P, Q) \in (\mathbb{R}_{n-1}[X])^2$.

$$\langle P; Q\rangle = \int_0^1 P(t)Q(t)dt = \int_0^1 Q(t)P(t)dt = \langle Q; P\rangle$$

— *Bilinéarité* :
Soient $(P_1, P_2, Q) \in (\mathbb{R}_{n-1}[X])^3$ et $\lambda \in \mathbb{R}$.

$$\langle P_1+\lambda P_2; Q\rangle = \int_0^1 (P_1+\lambda P_2)(t)Q(t)dt = \int_0^1 P_1(t)Q(t)dt+\lambda\int_0^1 P_2(t)Q(t) = \langle P_1; Q\rangle+\lambda P_2; Q\rangle$$

— *Positivité* :
Soit $P \in \mathbb{R}_{n-1}[X]$.

$$\langle P; P\rangle = \int_0^1 P^2(t)dt \geq 0$$

car $t \mapsto P(t)^2$ est positive sur $[0, 1]$.

— *Définie positive* :
Soit $P \in \mathbb{R}_{n-1}[X]$ tel que $\langle P; P\rangle$. La fonction $t \mapsto P(t)^2$ est continue et positive sur $[0, 1]$ donc puisque l'intégrale est nulle, on en déduit que la fonction est nulle.

Donc $\langle ; \rangle$ est un produit scalaire.

2. On en déduit aisément que H est symétrique réelle.
On pose $P_i = X^i$ pour tout $i \in \mathbb{N}$.
On remarque que pour tout $(i,j) \in \mathbb{N}^2$,

$$\langle P_i, P_j \rangle = \frac{1}{i+j+1}$$

Ainsi, on peut donc réécrire H comme étant la matrice des coefficients $(\langle P_i; P_j \rangle)$.

Soit $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathcal{M}_{n,1}(\mathbb{R})$

$$\begin{aligned} X^\top H X &= \sum_{i=1}^{n}\sum_{j=0}^{n} x_i x_j \langle P_i, P_j \rangle \\ &= \langle \sum_{i=1}^{n} x_i P_i, \sum_{j=1}^{n} x_j P_j \rangle && \text{par bilinéarité du produit scalaire} \\ &= \|P\|^2 && \text{où} P = \sum_{i=0}^{n} x_i P_i \end{aligned}$$

Ainsi, on en déduit que H est définie positive.

XIII.10.11 Racine carrée d'un endomorphisme auto-adjoint positif

[Enoncé]

XIII.10.12 Inégalité de convexité

[Enoncé]
On note $\lambda_1, \dots, \lambda_n$ les valeurs à M notée avec répétition.
Puisque $M \in \mathcal{S}_n^+(\mathbb{R})$, on sait que pour tout $i \in [\![1;n]\!]$, $\lambda_i \geq 0$.
Si l'un des λ_i est nul, le résultat est vérifié immédiatement.
Supposons qu'ils sont tous non nuls, on a donc d'après l'inégalité arithmético-géométrique (Tome I : I-47)que :

$$\frac{1}{n}\sum_{i=1}^{n} \lambda_i \geq (\lambda_1 \dots \lambda_n)^{1/n}$$

i.e

$$\frac{\mathrm{Tr}(M)}{n} \geq \det(M)^{1/n}$$

XIII.10.13 Inégalité à propos des matrices orthogonales

[Enoncé]

XIII.10.14 Inégalité de la trace

[Enoncé]

XIII.10.15 Inégalité de Hadamard

[Enoncé]

XIII.10.16 Perturbations

[Enoncé]

XIII.10.17 Somme de Cesàro de matrices orthogonales

[Enoncé]

XIII.10.18 Transformation de Cayley

[Enoncé]

XIII.10.19 Optimisation (1)

[Enoncé]

XIII.10.20 Optimisation (2)

[Enoncé]

XIII.10.21 Optimisation (3)

[Enoncé]

XIII.10.22 Caractérisation des isométries anti-involutives

[Enoncé]

XIII.10.23 Symétrie de l'espace

[Enoncé]

XIII.10.24 Réflexion et rotation dans un plan ★★★

[Enoncé]

1. a. Soit s_1 et s_2 deux réflexions. Puisque $(\mathcal{O}(E), \circ)$ est un groupe $s_1 \circ s_2 \in \mathcal{O}(E)$
   On a : $\det(s_1) = \det(s_2) = -1$.
   Donc, $\det(s_1 \circ s_2) = 1$. Et puisque E est de dimension 2, on en déduit que $s_1 \circ s_2$ est une rotation.
   b. On note $\mathcal{B} = (e_1, e_2)$ une base orthonormée de E.
   Soit r une rotation d'angle θ du plan E.
   On pose s_1 la réflexion par rapport à $D_1 = \text{Vect}(\cos(\theta/2)e_1 + \sin(\theta/2)e_2)$ et s_2 la réflexion par rapport à $D_2 = \text{Vect}(\cos(3\theta/2)e_1 + \sin(3\theta/2)e_2)$. En étudiant les matrices de r et de $s_1 \circ s_2$ dans la base $\mathcal{B}$, on a $r = s_1 \circ s_2$.
2. Puisque $\mathcal{O}(E)$ est un groupe, $r \circ s$ est une isométrie vectorielle.
   On a : $\det(r \circ s) = -1$ donc $r \circ s$ est une réflexion.
   Ainsi, $(r \circ s)^2 = \text{Id}_E$ et donc on en déduit que : $\begin{cases} r \circ s \circ r = s^{-1} = s \\ s \circ r \circ s = r^{-1} \end{cases}$
3. Soient s une réflexion de E et r une rotation de E tel que $s \circ r = r \circ s$. Puisque s est une réflexion, on a $s = s^{-1}$, donc $s \circ r \circ s = r$.
   Or d'après la question précédente, $s \circ r \circ s = r^{-1}$, d'où $r = r^{-1}$. Et donc, $r = \text{Id}_E$ ou $r = -\text{Id}_E$.

XIII.10.25 Similitude entre matrices orthogonales

[Enoncé]

XIII.10.26 Propriété de l'adjoint

[Enoncé]

XIII.10.27 Autour de l'adjoint

[Enoncé]

XIII.10.28 Somme d'une matrice orthogonale et de sa transposée

[Enoncé]

XIII.10.29 Déterminant d'une exponentielle

[Enoncé]
On pose $Sp(A) = \{\lambda_1, \dots, \lambda_n\}$. On trigonalise A dans $\mathcal{M}_n(\mathbb{C})$ donc il existe $P \in \mathrm{GL}_n(\mathbb{C})$ et $T\mathcal{M}_n(\mathbb{C})$ triangulaire supérieure tel que $A = PTP^{-1}$. On sait que e^A est semblable à e^T par continuité de l'exponentielle matricielle.
Ainsi, $\det(e^A) = \det(e^T)$. Or $\det(e^T) = \prod_{i=1}^n e^{\lambda_i} = e^{\sum_{i=1}^n \lambda_i} = e^{\mathrm{Tr}(T)}$ Et pour finir, puisque A et T sont semblables, on en déduit le résultat :

$$\det(e^A) = e^{\mathrm{Tr}(A)}$$

XIII.10.30 Exponentielle de matrices antisymétrique

[Enoncé]

XIII.10.31 Théorème spectral

[Enoncé]

XIII.10.32 Réduction simultanée

[Enoncé]

XIII.10.33 Réduction des matrices antisymétriques

[Enoncé]

XIII.10.34 Caractérisation des matrices symétriques positives

[Enoncé]

XIII.10.35 Matrices entières positives

[Enoncé]

XIII.10.36 Matrices binaires positives

[Enoncé]

XIII.10.37 Inégalité de Hoffman-Wielandt

[Enoncé]

XIII.10.38 Distance aux matrices de rang au plus r

[Enoncé]

XIII.10.39 Théorème de Courant-Fischer ★★★

[Enoncé]
D'après le théorème spectral il existe une base orthonormée $\mathcal{B}_0 = (x_1, \dots, x_n)$ de E formée de vecteurs propres de u. On note pour $i \in [\![1; n]\!]$, λ_i la valeur propre associée à x_i. Fixons $p \in [\![1; n]\!]$ et notons $V_p = \text{Vect}(x_1, \dots, x_p)$.
$\forall x = \sum_{i=1}^{p} a_i x_i \in V_p \cap S$, $\langle u(x), x\rangle = \left\langle \sum_{i=1}^{p} a_i \lambda_i x_i, \sum_{j=1}^{p} a_j x_j \right\rangle = \sum_{i=1}^{p}\sum_{j=1}^{p} \lambda_i a_i a_j \langle x_i, x_j\rangle =$
$\sum_{k=1}^{p} \lambda_k a_k^2 \geq \lambda_p \sum_{k=1}^{p} a_k^2 = \lambda_p$.
Donc $\lambda_p = \inf_{x \in V_p \cap S} \langle u(x), x\rangle$.
Soit maintenant $V \in \mathcal{F}_p$. Il faut montrer que $\inf_{x \in V \cap S} \langle u(x), x\rangle \leq \inf_{x \in V_p \cap S} \langle u(x), x\rangle$, il suffit donc de montrer qu'il existe un vecteur unitaire $z \in V$ tel que $\langle u(z), z\rangle \leq \lambda_p$.
Notons $G_p = \text{Vect}(x_p, \dots, x_n)$. D'après la formule de Grassmann,
$\dim(V \cap G_p) = \dim(V) + \dim(G_p) - \dim(V + G_p) = n + 1 - \dim(V + G_p)$.
Or $V + G_p \subset E$ donc $\dim(V + G_p) \leq n$. Ainsi $\dim(V \cap G_p) \geq 1 : \exists y \in V \cap G_p \backslash \{0\}$. Posons $z = \frac{y}{\|y\|}$.
$z \in G_p$ donc il existe des scalaires $b_p, \dots, b_n$ tels que $z = \sum_{i=p}^{n} b_i x_i$. Alors $\langle u(z), z\rangle = \sum_{i=p}^{n} \lambda_i b_i^2 \leq$
$\lambda_p \sum_{i=p}^{n} b_i^2 = \lambda_p$.

On a donc montré que :

$$\lambda_p = \sup_{F\in\mathcal{F}_p}\left(\inf_{x\in F\cap S}\langle u(x),x\rangle\right)$$

Pour la deuxième égalité on peut refaire un raisonnement similaire ou alors on applique le résultat à $v=-u$.
v est autoadjoint et ses valeurs propres sont $-\lambda_n \geq \cdots \geq -\lambda_1$.
On sait alors que $-\lambda_p = \sup_{F\in\mathcal{F}_{n+1-p}}\left(\inf_{x\in F\cap S}\langle v(x),x\rangle\right) = \sup_{F\in\mathcal{F}_{n+1-p}}\left(-\sup_{x\in F\cap S}\langle u(x),x\rangle\right) = -\inf_{F\in\mathcal{F}_{n+1-p}}\left(\sup_{x\in F\cap S}\langle u(x),x\rangle\right)$.
Ainsi $\lambda_p = \inf_{F\in\mathcal{F}_{n+1-p}}\left(\sup_{x\in F\cap S}\langle u(x),x\rangle\right)$

XIII.10.40 Principe de Ky-Fan

[Enoncé]

XIII.10.41 Théorème de Cartan-Dieudonnée

[Enoncé]

XIII.10.42 Relation d'ordre des matrices symétriques

[Enoncé]

XIII.11 Correction Décompositions matricielles

XIII.11.1 Décomposition de Dunford ★★

[Enoncé]

1. On sait que $\chi_M = \prod_{\lambda \in \mathrm{Sp}(M)} (X-\lambda)^{m_\lambda}$.
   Si λ et μ sont deux valeurs propres distinctes de M alors $(X-\lambda)^{m_\lambda}$ et $(X-\mu)^{m_\mu}$ sont premiers entre eux.
   Ainsi d'après le lemme des noyaux, $\mathrm{Ker}(\chi_M(M)) = \bigoplus_{\lambda \in \mathrm{Sp(M)}} \mathrm{Ker}((M-\lambda I_n)^{m_\lambda})$.
   De plus d'après le théorème de Cayley-Hamilton, $\chi_M(M) = 0_n$. Ainsi,
   $$\mathbb{C}^n = \bigoplus_{\lambda \in \mathrm{Sp}(M)} F_\lambda$$

2. Notons u l'endomorphisme canoniquement associé à M. Si $\lambda \in \mathrm{Sp}(M)$, M et $(M-\lambda I_n)^{m_\lambda}$ commutent donc F_λ est stable par u. On note u_λ l'endomorphisme induit par u sur F_λ.
   On écrit alors $u_\lambda = \lambda \,\mathrm{Id}_{F_\lambda} + (u_\lambda - \lambda \,\mathrm{Id}_{F_\lambda})$. Par définition de $F_\lambda, (u_\lambda - \lambda \,\mathrm{Id}_{F_\lambda})^{m_\lambda} = 0$.
   Donc $n_\lambda = u - \lambda \,\mathrm{Id}_{F_\lambda}$ est nilpotent. On note N_λ la matrice de n_λ dans une base $\mathcal{B}_\lambda$ de F_λ.
   On note enfin $\mathrm{Sp}(M) = \{\lambda_1, \dots, \lambda_p\}$, $\alpha_i = \dim(F_{\lambda_i})$ pour tout $i \in [\![1;p]\!]$ et $\mathcal{B}$ la base de $\mathbb{C}^n$ obtenue par concaténation des bases $\mathcal{B}_{\lambda_1}, \dots, \mathcal{B}_{\lambda_p}$ dans cet ordre.
   On peut écrire $M = D + N$ avec les matrices diagonales par blocs
   $$D = P \begin{pmatrix} \lambda_1 I_{\alpha_1} & & & \\ & \ddots & 0 & \\ & & \lambda_i I_{\alpha_i} & \\ & 0 & & \ddots \\ & & & & \lambda_p I_{\alpha_p} \end{pmatrix} P^{-1} \text{ et } N = P \begin{pmatrix} N_{\lambda_1} & & & \\ & \ddots & 0 & \\ & & N_{\lambda_i} & \\ & 0 & & \ddots \\ & & & & N_{\lambda_p} \end{pmatrix} P^{-1}$$
   où P désigne la matrice de passage de la base $\mathcal{B}$ à la base canonique de $\mathbb{C}^n$. On peut alors affirmer que D est diagonalisable ($P^{-1}DP$ est diagonale), que N est nilpotente car $N^k = P \begin{pmatrix} N_{\lambda_1}^k & & & \\ & \ddots & 0 & \\ & & N_{\lambda_i}^k & \\ & 0 & & \ddots \\ & & & & N_{\lambda_p}^k \end{pmatrix} P^{-1} = 0$ pour k le ppcm des indices de

nilpotence de $N_{\lambda_1}, \dots, N_{\lambda_p}$ par exemple, et que N et D commutent :

$$DN = P \begin{pmatrix} \lambda_1 N_{\lambda_1} & & & & \\ & \ddots & & 0 & \\ & & \lambda_i N_{\lambda_i} & & \\ & 0 & & \ddots & \\ & & & & \lambda_p N_{\lambda_p} \end{pmatrix} P^{-1} = ND$$

3. Supposons que $M = D + N = D' + N'$ soient deux décompositions de Dunford de M. Alors $D - D' = N - N'$.
D et D' commutent car ce sont des polynômes en M. De même pour N et N'.
Alors comme D et D' sont diagonalisables, elle sont simultanément diagonalisables (cf. **??**). On en déduit que $D - D'$ est diagonalisable.
D'autre part, $N - N'$ est nilpotente. En effet comme N et N' commutent, si l'on note k et k' deux entiers naturels non nuls pour lesquels $N^k = {N'}^{k'} = 0$ alors on a :

$$(N-N')^{k'+k} = \sum_{i=0}^{k'+k} (-1)^i \binom{k'+k}{i} {N'}^i N^{k'+k-i} = \sum_{i=0}^{k'} (-1)^i \binom{k'+k}{i} {N'}^i N^{k'+k-i} + \sum_{i=k'+1}^{k'+k} (-1)^i \binom{$$

Or $\forall i \in [\![0; k']\!],\ k + k' - i \geq k \implies N^{k+k'-i} = 0$ et $\forall i \in [\![k'+1; k'+k]\!],\ i \geq k' \implies {N'}^i = 0$.
Donc $(N - N')^{k'+k} = 0$.
Ainsi $N - N' = D - D'$ est diagonalisable et nilpotente ce qui implique $D = D'$ et $N = N'$.

Diagonalisabilité de l'exponentielle d'une matrice ★★★

Supposons que A est diagonalisable. Alors il existe une matrice inversible P et une matrice diagonale $D = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$ telles que $A = PDP^{-1}$.

Posons pour $p \in \mathbb{N}$, $S_p = \sum_{k=0}^{p} \frac{A^k}{k!}$.

$$\forall p \in \mathbb{N},\ S_p = \sum_{k=0}^{p} \frac{PD^kP^{-1}}{k!} = P \left[\sum_{k=0}^{p} \operatorname{diag}\left(\frac{\lambda_1^k}{k!}, \dots, \frac{\lambda_n^k}{k!} \right) \right] P^{-1}.$$

Or l'application $M \in \mathcal{M}_n(\mathbb{C}) \mapsto PMP^{-1}$ est continue car linéaire sur $\mathcal{M}_n(\mathbb{C})$ qui est de dimension finie. Ainsi, $S_p \underset{p\to+\infty}{\longrightarrow} e^A$ et $\sum_{k=0}^{p} \operatorname{diag}\left(\frac{\lambda_1^k}{k!}, \dots, \frac{\lambda_n^k}{k!} \right) \underset{p\to+\infty}{\longrightarrow} \operatorname{diag}\left(e^{\lambda_1}, \dots, e^{\lambda_n}\right)$ donnent par passage à la limite $e^A = Pe^DP^{-1} = P \operatorname{diag}\left(e^{\lambda_1}, \dots, e^{\lambda_n}\right) P^{-1}$.
D'où e^A est diagonalisable.
Réciproquement supposons que e^A est diagonalisable. Par unicité de la décomposition de Dunford $e^A = D' + N'$ on sait que $D' = e^A$ et $N' = 0$.
On écrit la décomposition de Dunford $A = D + N$ de A et on va essayer de montrer que

$N = 0$. Pour cela on veut exprimer la décomposition de e^A en fonction de celle de A.

Comme D et N commutent on sait que $e^A = e^D e^N = e^D + e^D(e^N - I_n) = e^D + e^D \sum_{k=1}^{+\infty} \frac{N^k}{k!}$.

On sait déjà d'après ce qui a été fait précédemment que e^D est diagonalisable. De plus e^D et $e^D(e^N - I_n)$ commutent, il est alors naturel d'essayer de montrer que le deuxième terme est nilpotent.

Tout d'abord, en notant $p \geq 1$ l'indice de nilpotence de N on sait que $\sum_{k=1}^{+\infty} \frac{N^k}{k!} = \sum_{k=1}^{p-1} \frac{N^k}{k!}$.

Donc $e^D(e^N - I_n) = e^D N \sum_{k=1}^{p-1} \frac{N^{k-1}}{k!}$. Comme D et N commutent, e^D et N commutent et donc e^D commute avec tous les polynômes en N. Aussi, N commute avec tous les polynômes en N. Ainsi $\left(e^D(e^N - I_n)\right)^p = \left(e^D\right)^p N^p \left(\sum_{k=1}^{p-1} \frac{N^{k-1}}{k!}\right)^p = 0$.

Ainsi par unicité de la décomposition de Dunford, $e^D(e^N - I_n) = N' = 0$. Or on sait que $\det\left(e^D\right) = \det\left(\operatorname{diag}\left(e^{\lambda_1}, \dots, e^{\lambda_n}\right)\right) = \prod_{i=1}^{n} e^{\lambda_i} = \exp\left(\sum_{i=1}^{n} \lambda_i\right) = e^{\operatorname{Tr}(A)} > 0$. Donc e^D est inversible.

On en déduit que $e^N - I_n = 0$ i.e $e^N = I_n$ i.e $\sum_{k=1}^{p-1} \frac{N^k}{k!} = 0$. Or p étant l'indice de nilpotence de N on sait que le polynôme minimal de N est X^p. Le polynôme $P = \sum_{k=1}^{p-1} \frac{X^k}{k!}$ annule N et est de degré inférieur strictement à p, c'est donc le polynôme nul i.e $p = 1$ i.e $N = 0$.
Ainsi $A = D$ est diagonalisable.

Surjectivité de l'exponentielle matricielle ★★★★

1. Notons $M = D + N$ la décomposition de Dunford de M. On sait que $\operatorname{Sp}(M) = \operatorname{Sp}(D)$ donc D est inversible.
   Posons $U = I_n + D^{-1}N$ de sorte que $M = DU$. N et D commutent donc $\forall k \in \mathbb{N}^*$, $(D^{-1}N)^k = D^{-k}N^k$. Donc $D^{-1}N = U - I_n$ est nilpotente c'est à dire U est unipotente.
   D'après le résultat sur la décomposition de Dunford on sait que D et U commutent et que D est diagonalisable.
   Enfin, si $M = DU = D'U'$ sont deux décompositions de M alors $\det(M) \neq 0 \implies \det(U') \neq 0$ d'où $DD'^{-1} = U'U^{-1}$. De plus, on sait aussi que D, U, D', U' sont des polynômes en M. Ils commutent donc tous deux à deux. Ainsi D et D' sont codiagonalisables (cf. **??**) d'où DD'^{-1} est diagonalisable puis $I_n - DD'^{-1}$ est diagonalisable. De plus, $I_n - U'U^{-1} = (I_n - U')(U^{-1} - I_n) + 2I_n - U' - U^{-1} = (I_n - U')(I_n - U)U^{-1} + (I_n - U') + (U - I_n)U^{-1}$. Chacun des termes est une matrice nilpotente : $\forall k \in \mathbb{N}^*$, $\left((I_n - U')(I_n - U)U^{-1}\right)^k = (I_n - U')^k (I_n - U)^k U^{-k}$ et $\left((U - I_n)U^{-1}\right)^k =$

$(-1)^k(I_n-U)^kU^{-k}$.
Montrons que la somme de deux matrices nilpotentes A et B est nilpotente. On note $p,q\in\mathbb{N}^*$ tels que $A^p=B^q=0$. Alors,

$$(A+B)^{p+q}=\sum_{i=0}^{p+q}\binom{p+q}{i}A^iB^{p+q-i}=\sum_{i=0}^{p}\binom{p+q}{i}A^iB^{p+q-i}+\sum_{i=p+1}^{p+q}\binom{p+q}{i}A^iB^{p+q-i}$$

Or $\forall i\in[\![0;p]\!],\ p+q-i\geq q\implies B^{p+q-i}=0$ et $\forall i\in[\![p+1;p+q]\!],\ i\geq p\implies A^i=0$.
Donc $(A+B)p+q=0$.
Ainsi $(I_n-U')+(U-I_n)U^{-1}$ est nilpotente puis $I_n-U'U^{-1}$ est nilpotente.
Ainsi $I_n-DD'^{-1}=I_n-U'U^{-1}$ est diagonalisable et nilpotente d'où $DD'^{-1}=I_n$ et $U'U^{-1}=I_n$ c'est à dire $D=D'$ et $U=U'$.

2. Soit $M\in\mathcal{M}_n(\mathbb{C})$. M est trigonalisable donc il existe une matrice inversible P et une matrice triangulaire supérieure T telles que $M=PTP^{-1}$. On note $\lambda_1,\dots,\lambda_n$ les coefficients diagonaux de T. Par continuité de l'application linéaire $A\in\mathcal{M}_n(\mathbb{C})\mapsto PAP^{-1}$, $e^M=Pe^TP^{-1}$. Donc $\det(e^M)=\det(e^T)$ est le produit des coefficients diagonaux de e^T. Or le calcul montre que les coefficients diagonaux de e^T sont $e^{\lambda_1},\dots,e^{\lambda_n}$.
Ainsi $\det(M)=\prod_{i=1}^{n}e^{\lambda_i}=\exp\left(\sum_{i=1}^{n}\lambda_i\right)=e^{\mathrm{Tr}(M)}>0$. D'où $e^M\in\mathrm{GL}_n(\mathbb{C})$ et det est bien une application de $\mathcal{M}_n(\mathbb{C})$ dans $\mathrm{GL}_n(\mathbb{C})$.
Ensuite, donnons nous une matrice $M\in\mathrm{GL}_n(\mathbb{C})$. On écrit $M=\Delta U=U\Delta$ avec Δ diagonalisable et U unipotente. Supposons qu'il existe $A\in\mathcal{M}_n(\mathbb{C})$ telle que $e^A=M$. On écrit $A=D+N$. Comme D et N commutent on sait que $e^A=e^De^N=e^Ne^D$. On sait aussi qu'en notant $D=P\,\mathrm{diag}(\mu_1,\dots,\mu_n)P^{-1}$ on a $e^D=P\,\mathrm{diag}(e^{\mu_1},\dots,e^{\mu_n})P^{-1}$ qui est donc diagonalisable.
Enfin, notons p l'indice de nilpotence de N. on calcule $e^N=\sum_{k=0}^{+\infty}\frac{N^k}{k!}=I_n+\sum_{k=1}^{p-1}\frac{N^k}{k!}$.
Donc $I_n-e^N=-N\sum_{k=1}^{p-1}\frac{N^{k-1}}{k!}$. N commute avec $\sum_{k=1}^{p-1}\frac{N^{k-1}}{k!}$ qui est un polynôme en N.
donc I_n-e^N est nilpotente c'est à dire e^N est unipotente.
Par unicité de la décomposition de la question 1, $e^D=\Delta$ et $e^N=U$.
Il faut et suffit donc de choisir D et N qui commutent telles que $e^D=\Delta$ et $e^N=U$ puis de poser $A=D+N$.
Δ est diagonalisable on peut donc noter $\Delta=Q\,\mathrm{diag}(\lambda_1,\dots,\lambda_n)Q^{-1}$. Comme $\det(M)\neq 0$, $\det(\Delta)\neq 0$ c'est à dire $\forall i\in[\![1;n]\!],\ \lambda_i\neq 0$. Or on sait que $\exp:\mathbb{C}\to\mathbb{C}^*$ est surjective. On peut donc choisir pour tout $i\in[\![1;n]\!],\ \mu_i\in\mathbb{C}$ tel que $e^{\mu_i}=\lambda_i$. $D=P\,\mathrm{diag}(\mu_1,\dots,\mu_n)P^{-1}$ vérifie $e^D=\Delta$.
Ensuite, on écrit $U=I_n-(I_n-U)$. On va s'inspirer du développement du logarithme dans $\mathbb{R}$: $\forall x\in]-1,1[,\ \ln(1-x)=-\sum_{k=1}^{+\infty}\frac{x^k}{k}$.

On pose $N = \sum_{k=1}^{p-1} \frac{(I_n - U)^k}{k} = (I_n - U)\sum_{k=1}^{p-1} \frac{(I_n - U)^{k-1}}{k}$ où p désigne l'indice de nilpotence de $I_n - U$. Montrons que $e^N = U$.
On pose $F : x \mapsto \sum_{k=1}^{p-1} \frac{x^k}{k}$ et $G : x \mapsto \sum_{k=0}^{p-1} \frac{x^k}{k!}$.
On sait que $\ln(1-x) \underset{x\to 0}{=} F(x) + o(x^p)$ et $e^x \underset{x\to 0}{=} G(x) + o(x^p)$. Donc par composition $e^{\ln(1-x)} = 1 - x \underset{x\to 0}{=} G \circ F(x) + o(x^p)$ i.e $G \circ F(x) \underset{x\to 0}{=} 1 - x + o(x^p)$. Cette expression permet de connaître le développement du polynôme $G \circ F$ jusqu'au terme en X^p.
Ainsi, comme $(I_n - U)^p = 0$ on en déduit $e^N = G \circ F(I_n - U) = U$.
On pose enfin $A = D + N$, on sait que D et N commutent car $e^N = U$ commute avec $e^D = \Delta$ et par conséquent $e^A = e^D e^N = \Delta U = M$.
Remarque : On peut montrer de même que $F \circ G(I_n - U) = U$ et donc montrer que $M \mapsto \sum_{k=1}^{+\infty} \frac{M^k}{k}$ réalise une bijection des matrices nilpotentes dans les matrices unipotentes.

Opérateur de commutation ★★★

1. On note E_{ij} la matrice dont tous les coefficients sont nuls sauf celui en position (i,j) qui vaut 1. Fixons $(i,j) \in [\![1;n]\!]$.
$\mathrm{Comm}_A(PE_{ij}P^{-1}) = APE_{ij}P^{-1} - PE_{ij}P^{-1}A = PDE_{ij}P^{-1} - PE_{ij}P^{-1}DP^{-1} = P(DE_{ij} - E_{ij}D)P^{-1} = P(\lambda_i E_{ij} - \lambda_j E_{ij})P^{-1} = (\lambda_i - \lambda_j)PE_{ij}P^{-1}$.
Ainsi $(PE_{ij}P^{-1})_{1\le i,j\le n}$ est une famille de vecteurs propres de Comm_A. De plus, l'application $M \in \mathcal{M}_n(\mathbb{C}) \mapsto PMP^{-1}$ est un isomorphisme (de réciproque $M \in \mathcal{M}_n(\mathbb{C}) \mapsto P^{-1}MP$).
Donc comme $(E_{ij})_{1\le i,j\le n}$ est une base de $\mathcal{M}_n(\mathbb{C})$, $(PE_{ij}P^{-1})_{1\le i,j\le n}$ est une base de $\mathcal{M}_n(\mathbb{C})$.
Par conséquent Comm_A est diagonalisable.

2. On note $A = D + N$ la décomposition de Dunford de A.
On vérifie aisément que $\mathrm{Comm}_A = \mathrm{Comm}_D + \mathrm{Comm}_N$ et que $\mathrm{Comm}_D \mathrm{Comm}_N = \mathrm{Comm}_N \mathrm{Comm}_D$ (conséquence directe du fait que D et N commutent). On sait de plus d'après ce qui a été fait précédemment que D diagonalisable entraîne Comm_D diagonalisable.
Montrons que Comm_N est nilpotente. Fixons $B \in \mathcal{M}_n(\mathbb{C})$.
Montrons par récurrence sur $p \in \mathbb{N}^*$ qu'il existe des entiers $\beta_{p,0}, \dots, \beta_{p,p}$ (qui ne dépendent pas de B) tels que $\mathrm{Comm}_N^p(B) = \sum_{i=0}^{p} \beta_{p,i} N^{p-i} B N^i$.
$p = 1$:
$\mathrm{Comm}_N(B) = NB - BN = \sum_{i=0}^{1} N^{1-i} B N^i$. La propriété est vraie en posant $\beta_{1,0} = \beta_{1,1} =$

1. Supposons la propriété vraie à un certain rang $p \in \mathbb{N}^*$.

$$\begin{aligned}\mathrm{Comm}_N^{p+1}(B) &= N\left(\sum_{i=0}^{p}\beta_{p,i}N^{p-i}BN^i\right) - \left(\sum_{i=0}^{p}\beta_{p,i}N^{p-i}BN^i\right)N \\ &= \sum_{i=0}^{p}\beta_{p,i}N^{p+1-i}BN^i - \sum_{i=0}^{p}\beta_{p,i}N^{p-i}BN^{i+1} \\ &= \sum_{i=0}^{p}\beta_{p,i}N^{p+1-i}BN^i - \sum_{i=1}^{p+1}\beta_{p,i-1}N^{p+1-i}BN^i \\ &= \beta_{p,0}N^{p+1}B + \sum_{i=1}^{p}(\beta_{p,i}+\beta_{p,i-1})N^{p-i}BN^i + \beta_{p,p}BN^{p+1}\end{aligned}$$

On pose $\beta_{p+1,0} = \beta_{p,0},\ \beta_{p+1,p+1} = \beta_{p,p}$ et, $\forall i \in [\![1;p]\!],\ \beta_{p+1,i} = \beta_{p,i} + \beta_{p,i-1}$.
On a bien $\mathrm{Comm}_N^{p+1}(B) = \sum_{i=0}^{p+1}\beta_{p+1,i}N^{p+1-i}BN^i$ et $\forall i \in [\![0;p+1]\!],\ \beta_{p+1,i} \in \mathbb{Z}$.
On en déduit par récurrence simple que $\forall p \in \mathbb{N}^*,\ \exists(\beta_{p,0},\dots,\beta_{p,p}) \in \mathbb{Z}^{p+1},\ \mathrm{Comm}_A^p = B \in \mathcal{M}_n(\mathbb{C}) \mapsto \sum_{i=0}^{p}\beta_{p,i}N^{p-i}BN^i$.
Ainsi pour k l'indice de nilpotence de N, si $B \in \mathcal{M}_n(\mathbb{C})$, $\mathrm{Comm}_N^{2k}(B) = \sum_{i=0}^{k-1}\beta_{2k,i}N^{2k-i}BN^i + \sum_{i=k}^{2k}\beta_{2k,i}N^{2k-i}BN^i$.
Or $\forall i \in [\![1;k-1]\!],\ 2k-i \geq k \implies N^{2k-i} = 0$ et $\forall i \in [\![k;2k]\!],\ i \geq k \implies N^i = 0$.
Finalement $\mathrm{Comm}_N^{2k}(B) = 0$ quel que soit $B \in \mathcal{M}_n(\mathbb{C})$.
On en déduit que $\mathrm{Comm}_N^{2k} = 0$ et en particulier que Comm_N est nilpotente.
Ceci montre que $\mathrm{Comm}_A = \mathrm{Comm}_D + \mathrm{Comm}_N$ est la décomposition de Dunford de Comm_A.
Ainsi comme Comm_A est diagonalisable, Comm_N doit être nul.
Ceci impose que N doit commuter avec toutes les matrices de $\mathcal{M}_n(\mathbb{C})$.
N est donc une matrice scalaire $N = \alpha I_n$ (cf. I.6). Etant nilpotente, elle est nulle et $A = D$ est diagonalisable.

Deux applications non continues

XIII.11.2 Décomposition polaire ★★★

[Enoncé]

1. a. On remarque que $vu = v^3 = uv$. D'après le cours les sous-espaces propres de u sont stables par v. Notons pour $\lambda \in \mathrm{Sp}(u),\ E_\lambda = \mathrm{Ker}(u - \lambda\,\mathrm{Id}_E)$ et v_λ l'endomorphisme

induit par v sur E_λ. u est diagonalisable d'après le théorème spectral donc $\mathbb{C}^n = \bigoplus_{\lambda\in\mathrm{Sp}(u)} E_\lambda$. Fixons $\lambda \in \mathrm{Sp(u)}$.
d'après le théorème spectral v est diagonalisable et donc v_λ est diagonalisable. Soit μ une valeur propre de v_λ et x un vecteur propre associé.
$\mu^2 x = v_\lambda^2(x) = u(x) = \lambda x$. $\mu^2 = \lambda$. Or u et v sont autoadjoints définis positifs donc $\mu > 0$ et $\lambda > 0$. Ceci impose $\mu = \sqrt{\lambda}$.
Finalement v_λ est diagonalisable et admet pour seule valeur propre $\sqrt{\lambda}$. On en déduit que $v_\lambda = \sqrt{\lambda} I_{\dim(E_\lambda)}$.
On a déterminé v sur des sous-espaces supplémentaires dans $\mathbb{C}^n$. v est donc déterminé sur $\mathbb{C}^n$.

b. Notons $\mathrm{Sp}(u) = \{\lambda_1, \dots, \lambda_p\}$. On utilise les polynômes interpolateurs de Lagrange.
On pose pour $1 \leq j \leq p$, $L_j(X) = \prod_{\substack{1\leq i\leq n\\ i\neq j}} \frac{X-\lambda_i}{\lambda_j-\lambda_i}$ de sorte que $\forall j \in [\![1;p]\!]$, $L_j(\lambda_i) = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{sinon} \end{cases}$.
On vérifie alors que $v = \left(\sum_{j=1}^{p} \sqrt{\lambda_j} L_j\right)(u)$.

2. a. Tout d'abord, $\left(A^\top A\right)^\top = A^\top A$. Ensuite, si $X \in \mathbb{R}^n \backslash \{0\}$,
$X^\top A^\top A X = \|AX\|^2$ pour $\|.\| : Y \in \mathbb{R}^n \mapsto Y^\top Y$ la norme euclidienne usuelle sur $\mathbb{R}^n$.
Or $A \in \mathrm{GL}_n(\mathbb{R})$ donc $X \neq 0 \implies AX \neq 0 \implies \|AX\|^2 > 0$. Ainsi $A^\top A$ est une matrice symétrique définie positive.

b. Si $A = OS$ avec $(O,S) \in \mathcal{O}_n(\mathbb{R}) \times S_n^{++}(\mathbb{R})$ alors $A^\top A = S^\top O^\top O S = S^\top S = S^2$. Donc S est l'unique matrice de $S_n^{++}(\mathbb{R})$ qui vérifie $A^\top A = S^2$. On a alors forcément $O = AS^{-1}$.
On calcule $O^\top O = \left(S^{-1}\right)^\top A^\top A S^{-1} = \left(S^\top\right)^{-1} S = S^{-1} S = I_n$ donc O est bien une matrice orthogonale.

3. On sait que $\mathrm{GL}_n(\mathbb{R})$ est dense dans $\mathcal{M}_n(\mathbb{R})$ (cf. VIII-53 tome Analyse). On peut donc poser une suite $(A_k)_{k\in\mathbb{N}}$ de matrice inversible qui converge vers A. Pour tout $k \in \mathbb{N}$ on note $A_k = O_k S_k$ la décomposition polaire de A_k.
Comme $\mathcal{O}_n(\mathbb{R})$ est compact on peut extraire une suite $(O_{\varphi(k)})_{k\in\mathbb{N}}$ de $(O_k)_{k\in\mathbb{N}}$ qui converge. On note O sa limite.
$\forall k \in \mathbb{N}$, $S_{\varphi(k)} = O_{\varphi(k)}^{-1} A_{\varphi(k)}$.
On sait que l'application $M \in \mathcal{M}_n(\mathbb{R}) \mapsto M^{-1}$ est continue puisque les coefficients de M^{-1} sont polynomiaux en ceux de M. De plus $A_{\varphi(k)} \underset{k\to+\infty}{\longrightarrow} A$ comme suite extraite de $(A_k)_{k\in\mathbb{N}}$. Enfin l'application $(M,N) \in \mathcal{M}_n(\mathbb{R})^2 \mapsto MN$ est continue car bilinéaire sur $\mathcal{M}_n(\mathbb{R})$ qui est de dimension finie.
Ainsi par passage à la limite, $S_{\varphi(k)} \underset{k\to+\infty}{\longrightarrow} O^{-1} A = S$.

Or $(S_{\varphi(k)})_{k\in\mathbb{N}} \in S_n^+(\mathbb{R})^{\mathbb{N}}$. On sait que si $X \in \mathbb{R}^n$ alors $\forall k \in \mathbb{N},\ X^\top S_{\varphi(k)} X \geq 0$ et $S_{\varphi(k)}^\top = S_{\varphi(k)}$. Donc comme les applications $M \in \mathcal{M}_n(\mathbb{R}) \mapsto X^\top M X$ et $M \in \mathcal{M}_n(\mathbb{R}) \mapsto M^\top$ sont continues car linéaires, on obtient par passage à la limite : $X^\top S X \geq 0$ et $S^\top = S$. C'est à dire $S \in S_n^+(\mathbb{R})$.
Finalement, $A = OS$ où $(O, S) \in \mathcal{O}_n(\mathbb{R}) \times S_n^+(\mathbb{R})$.
Il n'y a pas unicité. Par exemple la matrice nulle peut s'écrire $0_n = I_n \times 0_n = -I_n \times 0_n$ où $(I_n, -I_n) \in \mathcal{O}_n(\mathbb{R})^2$ et $0_n \in S_n^+(\mathbb{R})$.

Sous-groupe compact maximal de $\mathbf{GL}_n(\mathbb{R})$ ★★★

1. Soit $A \in \mathcal{M}_n(\mathbb{R})$. Remarquons que $A^\top A \in S_n^+(\mathbb{R})$. En effet, $A^\top A$ est clairement symétrique et $\forall X \in \mathbb{R}^n,\ X^\top A^\top A X = \|AX\|_2^2 \geq 0$. On note alors $\lambda_1, \dots, \lambda_n$ les valeurs propres de $A^\top A$ comptées avec multiplicités et $e_1, \dots, e_n$ des vecteurs propres associés formant une base de $\mathbb{R}^n$. On sait que $\forall i \in [\![1; n]\!],\ \lambda_i \in \mathbb{R}_+$. Fixons $X = \sum_{i=1}^n a_i e_i \in \mathbb{R}^n$ tel que $\|X\|_2 = 1$. On a

$$0 \leq \|AX\|_2^2 = X^\top A^\top A X = \sum_{i=1}^n \lambda_i a_i^2 \leq \rho(A^\top A) \sum_{i=1}^n a_i^2 = \rho(A^\top A)\|X\|_2^2 = \rho(A^\top A)$$

   De plus, en notant $i_0 \in [\![1; n]\!]$ tel que $\lambda_{i_0} = \rho(A^\top A)$ on a $X^\top e_{i_0} X = \rho(A^\top A)$.
   Ainsi $|||A|||_2 = \sqrt{\rho(A^\top A)}$.
2. $\mathcal{O}_n(\mathbb{R})$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$:
   — $\mathcal{O}_n(\mathbb{R}) \subset \mathrm{GL}_n(\mathbb{R})$ $(\forall M \in \mathcal{O}_n(\mathbb{R}),\ M^{-1} = M^\top)$;
   — $I_n \in \mathcal{O}_n(\mathbb{R})$;
   — $\forall (A, B) \in \mathcal{O}_n(\mathbb{R})^2,\ (AB^{-1})^\top AB^{-1} = BA^\top AB^\top = BB^\top = I_n$.

   $\mathcal{O}_n(\mathbb{R})$ est compact :
   — $\mathcal{O}_n(\mathbb{R}) \subset \mathcal{M}_n(\mathbb{R})$ avec $\dim(\mathcal{M}_n(\mathbb{R})) = n^2 < +\infty$;
   — $\mathcal{O}_n(\mathbb{R}) = f^{-1}(\{I_n\})$ pour $f : M \mapsto M^\top M$ qui est continue car les coefficients de $f(M)$ sont polynomiaux en ceux de M. Donc $\mathcal{O}_n(\mathbb{R})$ est fermé ;
   — $\forall M \in \mathcal{O}_n(\mathbb{R}),\ |||M|||_2 = \sup_{\substack{X\in\mathbb{R}^n \\ \|X\|_2=1}} \|MX\|_2 = \sup_{\substack{X\in\mathbb{R}^n \\ \|X\|_2=1}} \|X\|_2 = 1$.

   $\mathcal{O}_n(\mathbb{R})$ est un fermé borné de $\mathcal{M}_n(\mathbb{R})$ qui est de dimension finie, c'est donc un compact.
3. a. Supposons que S ait une valeur propre $\lambda > 1$.
      Comme G est un groupe qui contient $\mathcal{O}_n(\mathbb{R})$, $\forall n \in \mathbb{N}^*,\ S^n = (O^{-1}A)^n \in G$.
      Nonobstant, $\forall n \in \mathbb{N}^*,\ \lambda^{2n} \in \mathrm{Sp}(S^{2n}) \implies \lambda^{2n} \leq \rho(S^{2n}) = |||S^n|||_2$. Ainsi $|||S^n|||_2 \underset{n\to+\infty}{\longrightarrow} +\infty$ ce qui est absurde puisque G est borné.
   b. Supposons que S ait une valeur propre $\lambda < 1$. Alors comme G est un groupe qui contient $\mathcal{O}_n(\mathbb{R})$, $S^{-1} = A^{-1}O \in G$. Or $\dfrac{1}{\lambda} \in \mathrm{Sp}(S^{-1})$ et $\dfrac{1}{\lambda} > 1$. Par le même raisonnement qu'à la question précédente ceci est absurde. On en déduit que $\mathrm{Sp}(S) = \{1\}$.

4. Le théorème spectral donne que S est diagonalisable. On a donc d'après la question précédente $S = I_n$.
Ainsi $A = O \in \mathcal{O}_n(\mathbb{R})$ et finalement $G = \mathcal{O}_n(\mathbb{R})$.

Enveloppe convexe des matrices orthogonales

1. Remarquons que $A^\top A \in S_n^+(\mathbb{R})$. En effet, $A^\top A$ est clairement symétrique et $\forall X \in \mathcal{M}_{n,1}(\mathbb{R}),\ X^\top A^\top AX = \|2\| AX^2 \geq 0$. On note alors $\lambda_1, \dots, \lambda_n$ les valeurs propres de $A^\top A$ comptées avec multiplicités et $e_1, \dots, e_n$ des vecteurs propres associés formant une base de $\mathcal{M}_{n,1}(\mathbb{R})$. On sait que $\forall i \in [\![1;n]\!],\ \lambda_i \in \mathbb{R}_+$. Fixons $X = \sum_{i=1}^{n} a_i e_i \in \mathcal{M}_{n,1}(\mathbb{R})$ tel que $\|X\|_2 = 1$. On a

$$0 \leq \|AX\|_2^2 = X^\top A^\top AX = \sum_{i=1}^{n} \lambda_i a_i^2 \leq \rho(A^\top A) \sum_{i=1}^{n} a_i^2 = \rho(A^\top A)\|X\|_2^2 = \rho(A^\top A)$$

De plus, en notant $i_0 \in [\![1;n]\!]$ tel que $\lambda_{i_0} = \rho(A^\top A)$ on a $X^\top e_{i_0} X = \rho(A^\top A)$.
Ainsi $|||A|||_2 = \sqrt{\rho(A^\top A)}$.

2. Soit $A \in \mathrm{Conv}(\mathcal{O}_n(\mathbb{R}))$. Il existe $A_1, \dots, A_p$ des matrices orthogonales ainsi que $t_1, \dots, t_p$ des réels positifs de somme 1 tels que $A = \sum_{i=1}^{p} t_i A_i$.
On remarque que $\forall M \in \mathcal{O}_n(\mathbb{R}),\ |||M|||_2 = \sup_{\substack{X \in \mathcal{M}_n(\mathbb{R}) \\ \|X\|_2 = 1}} \|MX\|_2 = \sup_{\substack{X \in \mathcal{M}_n(\mathbb{R}) \\ \|X\|_2 = 1}} \|X\|_2 = 1$.
Donc par inégalité triangulaire $|||A|||_2 \leq \sum_{i=1}^{p} t_i |||A_i|||_2 = \sum_{i=1}^{p} t_i = 1$ d'où $A \in \mathcal{B}$.

3. a. Soit $V \in \mathrm{Conv}(\mathcal{O}_n(\mathbb{R}))$.
D'une part, $\mathrm{Tr}(AV) - \mathrm{Tr}(AN) = \mathrm{Tr}(A(V-N)) = \langle M - N, V - N\rangle \leq 0$ d'après le théorème de projection sur un convexe compact.
D'autre part, $\mathrm{Tr}(AM) - \mathrm{Tr}(AN) = \mathrm{Tr}((M-N)^\top (M-N)) = \langle M-N, M-N\rangle \geq 0$. De plus $N \in \mathrm{Conv}(\mathcal{O}_n(\mathbb{R}))$ et $M \notin \mathrm{Conv}(\mathcal{O}_n(\mathbb{R}))$ donc $M \neq N$ d'où $\langle M-N, M-N\rangle > 0$.

   b. D'après la question précédente, pour $V = U^{-1} \in \mathcal{O}_n(\mathbb{R}) \subset \mathrm{Conv}(\mathcal{O}_n(\mathbb{R}))$, $\mathrm{Tr}(S) = \mathrm{Tr}(U^{-1}US) = \mathrm{Tr}(U^{-1}A) \leq \mathrm{Tr}(AN) < \mathrm{Tr}(AM) = \mathrm{Tr}(USM)$.

   c. D'après le théorème spectral il existe une base $(e_1, \dots, e_n)$ de $\mathcal{M}_{n,1}(\mathbb{R})$ formée de vecteurs propres de S. On note λ_i la valeur propre associée à e_i.

Points extrémaux des matrices orthogonales

Matrice extraite d'une matrice orthogonale

Matrices qui respectent le volume de k-parallélépipèdes rectangles

XIII.11.3 Décomposition QR

[Enoncé]

Matrice de Householder

XIII.11.4 Décomposition LU

[Enoncé]

$\mathbb{K} = \mathbb{R}$ **ou** $\mathbb{C}$

$\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$

Algorithme de calcul

Décomposition de Cholesky

XIII.11.5 Lemme de Fitting

[Enoncé]

XIII.11.6 Réduction de Jordan

[Enoncé]

1. On a : $\chi_M = \prod_{\lambda \in \mathrm{Sp}(M)} (X-\lambda)^{m_\lambda}$.
   Les polynômes $((X-\lambda)^{m_\lambda})_{\lambda \in \mathrm{Sp}(M)}$ sont premiers deux à deux.
   Donc d'après le lemme des noyaux, $\mathcal{M}_{n,1}(\mathbb{K}) = \bigoplus_{\lambda \in \mathrm{Sp}(M)} F_\lambda$.
2. Soit $(\alpha_0, \dots, \alpha_{p-1}) \in \mathbb{K}^p$ tel que

$$\sum_{i=0}^{p-1} \alpha_i f^i(x) = 0$$

   On note d le minimum de l'ensemble $\{i \in [\![0; p-1]\!] \, \alpha_i \neq 0\}$. Ce minimum existe car cet ensemble est une partie de $\mathbb{N}$.

On a donc $\sum_{i=d}^{p-1} \alpha_i f^i(x) = 0$. En composant par f^{p-1-d}, on a $\alpha_d f^{p-1}(x) = 0$.
Ainsi $\alpha_d = 0$, ce qui est absurde par définition de d.
Donc la famille $\mathcal{F}$ est libre. On a :

$$\mathrm{Mat}_{\mathcal{F}}(f) = J_p(0)$$

3. Soit $M \in \mathcal{M}_n(\mathbb{K})$ de polynôme caractéristique $\chi_M = \prod_{\lambda \in \mathrm{Sp}(M)} (X-\lambda)^{m_\lambda}$.
On note f l'endomorphisme canoniquement associé à M.
On remarque que $\varphi_\lambda = f_{|F_\lambda} - \lambda \mathrm{Id}$ est nilpotent d'indice m_λ sur F_λ pour tout $\lambda \in \mathrm{Sp}(M)$.
Donc $(\varphi_\lambda^{p-1}(x), \dots, \varphi_\lambda(x), x)$ est une base de F_λ. On a donc : $\mathrm{Mat}(\varphi_\lambda) = J_p(0)$ donc $\mathrm{Mat}(f_{|F_\lambda}) = J_p(\lambda)$.
On en déduit que M est semblable à une matrice diagonale par blocs de Jordan.

Application

XIII.11.7 Réduction de Frobenius

[Enoncé]

$M \sim M^\top$

Matrices semblables à leur inverse

Bicommutant

XIII.12 Correction Divers

XIII.12.1 Fonction $\mathbb{R}$-linéaire mais pas $\mathbb{C}$-linéaire ★

[Enoncé]

On pose $f : \left\{ \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \overline{z} \end{array} \right.$.

$\forall x, y \in \mathbb{C},\ \forall \lambda \in \mathbb{R},\ f(x + \lambda y) = \overline{x + \lambda y} = \overline{x} + \overline{\lambda}\overline{y} = f(x) + \lambda f(y)$.
Ainsi f est $\mathbb{R}$-linéaire.
Nonobstant $f(i \times 1) = -i \neq i = i \times f(1)$ donc f n'est pas $\mathbb{C}$-linéaire.

XIII.12.2 Relation d'ordre

[Enoncé]

XIII.12.3 Ordre lexicographique

[Enoncé]

XIII.12.4 Sous-groupes de $\mathrm{GL}_n(\mathbb{C})$ d'exposant fini ★★★★★

[Enoncé]
Soit $M \in G$.
$M^k = I_n$ donc les valeurs propres de M sont incluses dans l'ensemble des racines de $X^k - 1$ c'est à dire $\mathbb{U}_k$. On remarque aussi que M est diagonalisable ce qui servira plus tard.

Alors $T = \{\mathrm{Tr}(M),\ M \in G\} = \left\{ \sum_{\lambda \in \mathrm{Sp}(M)} m_\lambda(M)\lambda,\ M \in G \right\} \subset \left\{ \sum_{p=1}^{n} \lambda_p,\ (\lambda_1, \dots, \lambda_n) \in \mathbb{U}_k^n \right\}$.
Ce dernier ensemble étant fini car $\mathbb{U}_k$ l'est, T est fini.

Ensuite, Considérons $V = \mathrm{Vect}(G)$. V est de dimension finie comme sous-espace vectoriel de $\mathcal{M}_n(\mathbb{C})$ on peut donc en prendre une base $(M_1, \dots, M_d)$.

Posons alors l'application $f : \left\{ \begin{array}{ccc} G & \longrightarrow & T^d \\ M & \longmapsto & (\mathrm{Tr}(MM_1), \dots, \mathrm{Tr}(MM_d)) \end{array} \right.$ et montrons que f est injective.
Tout d'abord, f est bien une application. En effet, $\forall M \in G,\ \forall p \in [\![1; d]\!],\ M_p \in G \implies MM_p \in G$.
Fixons un couple de matrice $(A, B) \in G^2$ tel que $f(A) = f(B)$ c'est à dire $\forall p \in [\![1; d]\!],\ \mathrm{Tr}(AM_p) = \mathrm{Tr}(BM_p)$.

Alors par linéarité de la trace, pour toute combinaison linéaire $M = \sum_{p=1}^{d} x_p M_p,\ \mathrm{Tr}(AM) = \mathrm{Tr}(BM)$.

En particulier pour $B^{-1} \in G \subset V,\ \mathrm{Tr}(AB^{-1}) = \mathrm{Tr}(I_n) = n$.
Supposons alors par l'absurde que $A \neq B$ et donc que $C = AB^{-1} \neq I_n$. Alors le spectre de C n'est pas réduit à 1 (car sinon, C étant diagonalisable on aurait $C = I_n$). On note λ_0 une valeur propre de C différente de 1.
On a $\mathrm{Re}(\mathrm{Tr}(C)) = \mathrm{Re}(\lambda_0) + \sum_{\lambda \in \mathrm{Sp}(C)\setminus\{\lambda_0\}} \mathrm{Re}(\lambda) \leq \mathrm{Re}(\lambda_0) + \sum_{\lambda \in \mathrm{Sp}(C)\setminus\{\lambda_0\}} 1 = \mathrm{Re}(\lambda_0) + n - 1 < n$.
Ceci est absurde donc $A = B$.
On a donc construit une injection de G dans T^d qui est un ensemble fini. On en déduit que G est fini.

XIII.12.5 Formule de Burnside ★★★★

[Enoncé]
Toutes les sommes écrites sont des sommes **finies**.
Posons $\varphi = \frac{1}{|G|}\sum_{g\in G} g$. On veut montrer que $\mathrm{Tr}(\varphi) = \dim(V^G)$.
Le résultat paraît improbable dans le sens où $\mathrm{Tr}(\varphi) \in \mathbb{K}$. Et pourtant on doit montrer que $\mathrm{Tr}(\varphi)$ est un entier positif. Parmi les endomorphismes connus on sait que les projecteur ont une trace entière (égale à leur rang). On va donc essayer de montrer que φ est un projecteur.
On calcule $\varphi^2 = \left(\frac{1}{|G|}\sum_{g\in G} g\right)\left(\frac{1}{|G|}\sum_{h\in G} h\right) = \frac{1}{|G|^2}\sum_{g\in G}\sum_{h\in G} gh$.
Or pour tout $g \in G$ l'application $f_g : h \in G \mapsto gh$ est bijective. En effet, sa bijection réciproque est $f_{g^{-1}}$.
Donc $\varphi^2 = \frac{1}{|G|^2}\sum_{g\in G}\sum_{h\in G} f_g(h) = \frac{1}{|G|^2}\sum_{g\in G}\sum_{h\in G} h = \frac{1}{|G|^2}\sum_{h\in G}\sum_{g\in G} h = \frac{1}{|G|}\sum_{h\in G} h = \varphi$.
On sait alors que $\mathrm{Tr}(\varphi) = \mathrm{rg}(\varphi)$ et que $\mathrm{Im}(\varphi) = \mathrm{Ker}(\varphi - \mathrm{Id}_V)$. Ensuite si $x \in V^G$ alors $\varphi(x) = \frac{1}{|G|}\sum_{g\in G} g(x) = \frac{1}{|G|}\sum_{g\in G} x = x$ c'est à dire $x \in \mathrm{Ker}(\varphi - \mathrm{Id}_V)$. Donc $V^G \subset \mathrm{Im}(\varphi)$.
Réciproquement, donnons nous $x \in \mathrm{Im}(\varphi)$ et fixons $h \in G$.
On a $x = \frac{1}{|G|}\sum_{g\in G} g(x)$ donc $h(x) = \frac{1}{|G|}\sum_{g\in G} f_h(g)(x) = \frac{1}{|G|}\sum_{g\in G} g(x) = x$.
Ainsi $\mathrm{Im}(\varphi) = V^G$.
Finalement $\dim(V^G) = \mathrm{rg}(\varphi) = \mathrm{Tr}(\varphi) = \frac{1}{|G|}\sum_{g\in G} \mathrm{Tr}(g)$.

XIII.12.6 Théorème de Fermat matriciel

[Enoncé]

XIII.12.7 Développement décimal propre d'un réel

[Enoncé]

Une caractéristique des rationnels

XIII.12.8 Distribution du premier chiffre des puissances de 2

[Enoncé]