On a alors

$$\int_0^{+\infty} \frac{\mathrm{d}x}{x^2+\alpha x+1} = \frac{1}{x_1-x_0}\left[\ln\left(\frac{x-x_0}{x-x_1}\right)\right]_0^{+\infty} = \frac{1}{\sqrt{\Delta}}\ln\frac{\alpha+\sqrt{\Delta}}{\alpha-\sqrt{\Delta}}.$$

Exercice 27 : [énoncé]

(a) Posons $u_n(x) = 1/n^x$ définie sur $]1\,;+\infty[$.
La série de fonctions $\sum u_n$ converge simplement sur $]1\,;+\infty[$ ce qui assure la bonne définition de $\zeta(x)$.
Plus précisément, pour $a>1$, on a

$$\sup_{x\in[a;+\infty[}\left|u_n(x)\right| = u_n(a) \text{ avec } \sum u_n(a) \text{ convergente}$$

et il y a donc convergence normale (et donc uniforme) de la série de fonctions u_n sur $[a\,;+\infty[$.
Puisque

$$u_n(x) \xrightarrow[x\to+\infty]{} \begin{cases} 1 & \text{si } n=1 \\ 0 & \text{si } n\geq 2 \end{cases}$$

on peut appliquer le théorème de la double limite et affirmer que ζ tend en $+\infty$ vers la somme convergente des limites

$$\zeta(x) \xrightarrow[x\to+\infty]{} 1.$$

(b) Posons $v_n(x) = \zeta(n)x^n/n$. Pour $x\neq 0$, on a

$$\left|\frac{v_{n+1}(x)}{v_n(x)}\right| \xrightarrow[n\to+\infty]{} |x|.$$

Par le critère de d'Alembert, la série converge pour $|x|<1$ et diverge pour $|x|>1$ (en fait le rayon de convergence de cette série entière vaut 1).
Pour $x=1$, il y a divergence car

$$\frac{\zeta(n)}{n} \sim \frac{1}{n}.$$

Pour $x=-1$, il y a convergence en vertu du critère spécial des séries alternées. En effet, la suite $\big((-1)^n\zeta(n)/n\big)$ est alternée et décroît en valeur absolue vers 0 notamment car $\zeta(n+1)\leq\zeta(n)$.

(c) En tant que somme d'une série entière de rayon de convergence 1, la fonction F est assurément de classe $\mathcal{C}^1$ (et même $\mathcal{C}^\infty$) sur $]-1\,;1[$.
Les fonctions v_n sont continues sur $[-1\,;0]$ et l'on vérifie que la série $\sum v_n(x)$ satisfait le critère spécial des séries alternées pour tout $x\in[-1\,;0]$. On peut alors majorer le reste de cette série par son premier terme

$$\left|\sum_{k=n+1}^{+\infty} v_k(x)\right| \leq \left|v_{n+1}(x)\right| \leq \frac{\zeta(n)}{n}.$$

Ce dernier majorant étant uniforme de limite nulle, on peut affirmer qu'il y a convergence uniforme de la série de fonctions $\sum v_n$ sur $[-1\,;0]$ et sa somme F est donc continue.

(d) Par dérivation de la somme d'une série entière, on obtient pour $x\in]-1\,;1[$,

$$F'(x) = \sum_{n=1}^{+\infty}\zeta(n+1)x^n = \sum_{n=1}^{+\infty}\sum_{p=1}^{+\infty}\frac{x^n}{p^{n+1}}.$$

On peut permuter les deux sommes par le théorème de Fubini car il y a convergence des séries

$$\sum_{p\geq 1}\left|\frac{x^n}{p^{n+1}}\right| \text{ et } \sum_{n\geq 1}\sum_{p=1}^{+\infty}\left|\frac{x^n}{p^{n+1}}\right|.$$

On en déduit après sommation géométrique

$$F'(x) = \sum_{p=1}^{+\infty}\sum_{n=1}^{+\infty}\frac{x^n}{p^{n+1}} = \sum_{p=1}^{+\infty}\frac{x}{p(p-x)} = \sum_{p=1}^{+\infty}\left(\frac{1}{p-x}-\frac{1}{p}\right).$$

La série de fonction associée converge normalement sur tout segment de $]-1\,;1[$ et on peut donc intégrer terme à terme

$$F(x) = F(0)+\int_0^x F'(t)\,\mathrm{d}t = \int_0^x\sum_{p=1}^{+\infty}\left(\frac{1}{p-t}-\frac{1}{p}\right)\mathrm{d}t$$
$$= \sum_{p=1}^{+\infty}\int_0^x \frac{1}{p-t}-\frac{1}{p}\,\mathrm{d}t = \sum_{p=1}^{+\infty}\ln\left(\frac{p}{p-x}\right)-\frac{x}{p}.$$

Exercice 28 : [énoncé]
Remarquons que pour tout $t\in[0\,;1]$,

$$t-t^2\in[0\,;1/4].$$

(a) Pour $0 < r < R$, il y a absolument convergence de $\sum a_n r^n$. On a

$$\left|f(re^{i\theta})\right|^2 = \sum_{n=0}^{+\infty} a_n r^n e^{in\theta} \sum_{n=0}^{+\infty} \overline{a_n} r^n e^{-in\theta}.$$

Par produit de Cauchy de séries absolument convergentes, on obtient

$$\left|f(re^{i\theta})\right|^2 = \sum_{n=0}^{+\infty} \sum_{k=0}^{n} a_k \overline{a_{n-k}} e^{i(2k-n)\theta} r^n.$$

Puisque $\sum |a_n r^n|$ et $\sum |\overline{a_n} r^n|$ sont absolument convergentes, par produit de Cauchy, on peut affirmer que $\sum \sum_{k=0}^{n} |a_k| \, |\overline{a_{n-k}}| r^n$ converge. On en déduit que la série des fonctions continues $\theta \mapsto \sum_{k=0}^{n} a_k \overline{a_{n-k}} e^{i(2k-n)\theta} r^n$ est normalement convergente et donc on peut permuter somme et intégration :

$$\int_0^{2\pi} \left|f(re^{i\theta})\right|^2 d\theta = \sum_{n=0}^{+\infty} \int_0^{2\pi} \sum_{k=0}^{n} a_k \overline{a_{n-k}} e^{i(2k-n)\theta} r^n \, d\theta.$$

Or $\int_0^{2\pi} e^{ip\theta} \, d\theta = 0$ pour tout $p \in \mathbb{Z}^*$ donc, après simplification des termes nuls,

$$\frac{1}{2\pi} \int_0^{2\pi} \left|f(re^{i\theta})\right|^2 d\theta = \sum_{m=0}^{+\infty} |a_m|^2 r^{2m}.$$

(b) Pour $0 < r < R$ suffisamment petit

$$\sum_{n=1}^{+\infty} |a_n|^2 r^{2n} = \sum_{n=0}^{\infty} |a_n| r^{2n} - |a_0|^2 = \frac{1}{2\pi} \int_0^{2\pi} \left|f(re^{i\theta})\right|^2 - \left|f(0)\right|^2 d\theta.$$

Par intégration, d'une fonction négative, on obtient $\sum_{n=1}^{+\infty} |a_n|^2 r^{2n} \leq 0$. Or il s'agit d'une somme de termes positifs, ils sont donc tous nuls et on en déduit

$$\forall n \in \mathbb{N}^*, a_n = 0.$$

La fonction f est alors constante.

(c) Posons

$$f_N(z) = \sum_{n=0}^{N} a_n z^n.$$

Pour tout $r > 0$,

$$\sum_{n=N+1}^{+\infty} |a_n|^2 r^{2n} = \sum_{n=0}^{+\infty} |a_n|^2 r^{2n} - \sum_{n=0}^{N} |a_n|^2 r^{2n} = \frac{1}{2\pi} \int_0^{2\pi} \left|f(re^{i\theta}) - f_N(re^{i\theta})\right|^2 d\theta.$$

Pour $p \geq N+1$, on obtient

$$\sum_{n=N+1}^{+\infty} |a_n|^2 \frac{r^{2n}}{r^{2p}} = \frac{1}{2\pi} \int_0^{2\pi} \frac{\left|f(re^{i\theta}) - f_N(re^{i\theta})\right|^2}{r^{2p}} d\theta.$$

Or

$$0 \leq \int_0^{2\pi} \frac{\left|f(re^{i\theta}) - f_N(re^{i\theta})\right|^2}{r^{2p}} d\theta \leq 2\pi \frac{\left(P(r)\right)^2 + \left(\sum_{n=0}^{N} |a_n| r^n\right)^2}{r^{2p}} = \frac{O(r^{2N})}{r^{2p}}$$

donc

$$\frac{1}{2\pi} \int_0^{2\pi} \frac{\left|f(re^{i\theta}) - f_N(re^{i\theta})\right|^2}{r^{2p}} d\theta \xrightarrow[r \to +\infty]{} 0.$$

Pour $p = N+1$,

$$\sum_{n=N+1}^{+\infty} |a_n|^2 \frac{r^{2n}}{r^{2p}} = |a_{N+1}|^2 + \sum_{n=N+2}^{+\infty} |a_n|^2 r^{2(n-N-1)}$$

avec

$$0 \leq \sum_{n=N+2}^{+\infty} |a_n|^2 r^{2(n-N-1)} \leq \frac{1}{r^2} \sum_{n=N+2}^{+\infty} |a_n|^2 \xrightarrow[r \to +\infty]{} 0.$$

On en déduit $a_{N+1} = 0$ puis, en reprenant la démarche avec $p = N+2, \ldots$, on obtient successivement $a_{N+2} = 0, \ldots$ et finalement $f = f_N \in \mathbb{C}_N[X]$

Exercice 56 : [énoncé]
Notons $\sum a_n z^n$ la série entière dont la somme est égale à f sur B°.
La fonction f est continue sur un compact donc uniformément continue.
Pour tout $\varepsilon > 0$, il existe $\delta > 0$ vérifiant

$$\forall z, z' \in B, |z - z'| \leq \delta \implies \left|f(z) - f(z')\right| \leq \varepsilon.$$

Considérons alors $r = 1 - \delta$ et $g_r : z \mapsto f(rz)$.
Pour tout $z \in B$, $|z - rz| = \delta |z| \leq \delta$ donc $\left|f(z) - g(z)\right| \leq \varepsilon$. Ainsi $\|f - g\|_{\infty,B} \leq \varepsilon$
Puisque la série entière $\sum a_n z^n$ converge uniformément vers f sur tout compact inclus dans B°, la série entière $\sum a_n r^n z^n$ converge uniformément vers g sur B. Il existe donc un polynôme P vérifiant $\|P - g\|_{\infty,B} \leq \varepsilon$ puis $\|f - P\|_{\infty,B} \leq 2\varepsilon$ ce qui permet de conclure.

En développant la puissance

$$\sum_{n=0}^{+\infty} \mathrm{P}(T>n) = 5\sum_{n=0}^{+\infty}\left(\frac{5}{6}\right)^n - 10\sum_{n=0}^{+\infty}\left(\frac{5}{6}\right)^{2n} + 10\sum_{n=0}^{+\infty}\left(\frac{5}{6}\right)^{3n} - 5\sum_{n=0}^{+\infty}\left(\frac{5}{6}\right)^{4n} + \sum_{n=0}^{+\infty}\left(\frac{5}{6}\right)^{5n}$$

avec convergence des séries écrites.
Finalement

$$\mathrm{E}(T) = \sum_{k=1}^{5}(-1)^{k-1}\binom{5}{k}\frac{1}{1-(5/6)^k}.$$

Exercice 24 : [énoncé]
Une matrice de la forme

$$\begin{pmatrix} a & 1 \\ 0 & b \end{pmatrix}$$

est diagonalisable si $a \neq b$ (2 valeurs propres distinctes pour une matrice de taille 2) et ne l'est pas si $a = b$ (1 seule valeur propre et n'est pas une matrice scalaire).
La probabilité recherchée n'est donc autre que

$$\mathrm{P}(X \neq Y).$$

L'événement $(X \neq Y)$ est le complémentaire de l'événement $(X = Y)$ qui est la réunion d'événements deux à deux disjoints

$$(X=Y) = \bigcup_{n\in\mathbb{N}^*} (X=n, Y=n).$$

Par indépendance

$$\mathrm{P}(X=n, Y=n) = \mathrm{P}(X=n)\mathrm{P}(Y=n) = pq\big((1-p)(1-q)\big)^{n-1}.$$

Ainsi

$$\mathrm{P}(X=Y) = \frac{pq}{p+q-pq}.$$

Finalement, la probabilité que la matrice soit diagonalisable vaut

$$1-\mathrm{P}(X=Y) = \frac{p+q-2pq}{p+q-pq}.$$

Exercice 25 : [énoncé]

(a) Pour $s \leq t$, l'événement $A(0,0,s)$ contient l'événement $A(0,0,t)$ et donc $p_0(s) \geq p_0(t)$.
Pour $s, t \geq 0$, l'événement $A(0,0,s+t)$ est la conjonction des événements $A(0,0,s)$ et $A(0,s,s+t)$. Par conséquent

$$\mathrm{P}(A(0,0,s+t) = \mathrm{P}\big(A(0,0,s) \cap A(0,s,s+t)\big).$$

Par indépendance (hypothèse H1)

$$\mathrm{P}\big(A(0,0,s+t)\big) = \mathrm{P}\big(A(0,0,s)\big)\mathrm{P}\big(A(0,s,s+t)\big).$$

Or, l'hypothèse H2 donne $\mathrm{P}\big(A(0,s,s+t)\big) = \mathrm{P}(A(0,0,t))$ et donc

$$p_0(s+t) = p_0(s)p_0(t).$$

(b) Par l'hypothèse H3, la fonction p_0 prend la valeur 1 en 0 et est continue. Si par l'absurde cette fonction prend une valeur négative, elle s'annule en un certain $t_0 > 0$. L'équation fonctionnelle obtenue ci-dessus donne par une récurrence rapide

$$\forall k \in \mathbb{N}, \forall t \in \mathbb{R}, p_0(kt) = p_0(t)^k.$$

En prenant $t = t_0/k$, on obtient

$$\forall k \in \mathbb{N}^*, p_0(t_0/k) = 0.$$

En passant à limite quand k tend vers l'infini, on obtient l'absurdité $p_0(0) = 0$!
Puisqu'il est maintenant acquis que la fonction p_0 est à valeurs strictement positives, on peut introduire la fonction $f : \mathbb{R}_+ \to \mathbb{R}$ définie par

$$\forall t \in \mathbb{R}_+, f(t) = \ln\big(p_0(t)\big).$$

L'équation fonctionnelle obtenue en a) se traduit

$$\forall s, t \in \mathbb{R}_+, f(s+t) = f(s) + f(t).$$

Sachant la fonction f continue, on peut affirmer que celle-ci est linéaire : il existe $a \in \mathbb{R}$ tel que

$$\forall t \in \mathbb{R}_+, f(t) = at.$$

Ainsi,

$$\forall t \in \mathbb{R}_+, p_0(t) = \mathrm{e}^{at}.$$

Enfin, puisque la fonction p_0 est décroissante, le réel a est nécessairement négatif ce qui permet de l'écrire $-\lambda$ avec $\lambda \in \mathbb{R}_+$.

(c) Par l'hypothèse H5 avec $p_0(t) \underset{t\to 0^+}{=} 1-\lambda t+\mathrm{o}(t)$, on obtient

$$p_1(t)+\mathrm{o}(p_1(t)) \underset{t\to 0^+}{=} \lambda t+\mathrm{o}(t).$$

Ainsi $p_1(t) \underset{t\to 0^+}{\sim} \lambda t$ ce qui peut encore s'écrire

$$p_1(t) \underset{t\to 0^+}{=} \lambda t+\mathrm{o}(t).$$

Aussi, l'hypothèse H4 permet d'affirmer

$$\forall n\geq 2, p_n(t)\leq 1-p_0(t)-p_1(t) \underset{t\to 0^+}{=} \mathrm{o}(t)$$

et donc $p_n(t) \underset{t\to 0^+}{=} \mathrm{o}(t)$ pour tout $n\geq 2$.

(d) L'événement $A(n,0,s+t)$ est la réunion des événements deux à deux disjoints

$$A(k,0,s)\cap A(n-k,s,s+t) \text{ pour } k\in[\![0\,;n]\!].$$

On en déduit par additivité et les hypothèses H1 et H2 l'identité

$$p_n(s+t)=\sum_{k=0}^{n}\mathrm{P}(A(k,0,s))\mathrm{P}(A(n-k,s,s+t))=\sum_{k=0}^{n}p_k(s)p_{n-k}(t).$$

Cette identité fournit le développement asymptotique

$$p_n(t+s) \underset{s\to 0^+}{=} (1-\lambda s+\mathrm{o}(s))p_n(t)+\lambda s p_{n-1}(t)+\mathrm{o}(s)$$

car

$$p_0(s) \underset{s\to 0^+}{=} 1-\lambda s+\mathrm{o}(s), p_1(s) \underset{s\to 0^+}{=} \lambda s+\mathrm{o}(s) \text{ et } p_k(s) \underset{s\to 0^+}{=} \mathrm{o}(s) \text{ pour } k\geq 2.$$

On obtient alors

$$\frac{1}{s}\big(p_n(t+s)-p_n(t)\big) \underset{s\to 0^+}{=} \lambda p_{n-1}(t)-\lambda p_n(t)+\mathrm{o}(1).$$

On en déduit que la fonction p_n est dérivable et

$$p_n'(t)=\lambda(p_{n-1}(t)-p_n(t)).$$

(e) En introduisant $q_n(t)=\mathrm{e}^{\lambda t}p_n(t)$, on constate

$$q_0(t)=1 \text{ et } q_n'(t)=\lambda q_{n-1}(t).$$

Par récurrence

$$q_n(t)=\frac{(\lambda t)^n}{n!}$$

puis

$$\forall n\in\mathbb{N}, \forall t\in\mathbb{R}_+, p_n(t)=\mathrm{e}^{-\lambda t}\frac{(\lambda t)^n}{n!}.$$

(f) L'événement $(X=n)$ a la probabilité de l'événement $A(n,0,T)$ et donc

$$\mathrm{P}(X=n)=p_n(T)=\mathrm{e}^{-\lambda T}\frac{(\lambda T)^n}{n!}.$$

La variable X suit une loi de Poisson de paramètre λT. L'espérance de X vaut alors λT et le paramètre λ se comprend comme le nombre moyen de clients entrant par unité de temps.

Exercice 26 : [énoncé]

(a) Pour $(n,k)\in\mathbb{N}^2$. Si $k\leq n$ alors

$$\begin{aligned}\mathrm{P}(X=n,Y=k)&=\mathrm{P}(X=n)\mathrm{P}(Y=k\,|\,X=n)\\&=\mathrm{e}^{-\lambda}\frac{\lambda^n}{n!}\binom{n}{k}p^k(1-p)^{n-k}.\end{aligned}$$

Si $k>n$ alors $\mathrm{P}(X=n,Y=k)=0$.

(b) Pour $k\in\mathbb{N}$

$$\mathrm{P}(Y=k)=\sum_{n=0}^{+\infty}\mathrm{P}(X=n,Y=k)=\sum_{n=k}^{+\infty}\mathrm{P}(X=n,Y=k).$$

Après réorganisation et glissement d'indice

$$\mathrm{P}(Y=k)=\frac{(\lambda p)^k}{k!}\mathrm{e}^{-\lambda}\sum_{n=0}^{+\infty}\frac{1}{n!}(1-p)^n\lambda^n=\mathrm{e}^{-\lambda p}\frac{(\lambda p)^k}{k!}.$$

La variable Y suit une loi de Poisson de paramètre λp.

Exercice 27 : [énoncé]

(a) La loi conjointe de X et Y déterminant une probabilité

$$\sum_{j=0}^{+\infty}\sum_{k=0}^{+\infty}\mathrm{P}(X=j,Y=k)=1.$$

Or

$$\sum_{j=0}^{+\infty}\sum_{k=0}^{+\infty}\mathrm{P}(X=j,Y=k)=a\mathrm{e}^2$$

donc $a=\mathrm{e}^{-2}$.

Supposons que A soit définie positive. En notant e_i les vecteurs de la base canonique, on vérifie aisément que :

$$a_{i,i} = \langle Ae_i, e_i \rangle > 0, \quad 1 \leq i \leq n$$

Exercice 5 Densité de matrices

1) Soit $M \in M_n(\mathbb{K})$ et $\epsilon > 0$. On pose alors $M_k = M - \frac{1}{k} I_n$. On a pour k assez grand $M_k \in B(M, \epsilon)$. De plus les valeurs propres de M_k sont les $\lambda_k - \frac{1}{k}$. On en déduit que pour k assez grand, M_k n'admet pas 0 pour valeurs propres et donc M_k est inversible. Comme $M_k \in B(M, \epsilon)$, on en déduit que $GL_n(\mathbb{K})$ est dense dans $M_n(\mathbb{K})$.

2) Soit $A \in M_n(\mathbb{C})$, on sait que A est trigonalisable donc il existe $P \in GL_n(\mathbb{C})$ et T triangulaire supérieure telles que $A = PTP^{-1}$. On note λ_i les valeurs propres de A (sans répétition) et qui sont également les coefficients diagonaux de T. On pose $0 < \epsilon < \min_{i \neq j} |\lambda_i - \lambda_j|$ et $T_\epsilon = T + diag(\frac{\epsilon}{1}, \cdots, \frac{\epsilon}{n})$. On vérifie que T_ϵ n'a que des coefficients différents. En effet, si $\lambda_i + \frac{\epsilon}{s} = \lambda_j + \frac{\epsilon}{r}$ avec $s < r$, on a alors :

$$|\lambda_i - \lambda_j| = \epsilon |\frac{1}{s} - \frac{1}{r}| \leq \epsilon (1 - \frac{1}{r}) < \epsilon$$

Ce qui est absurde par définition de ϵ. Les valeurs propres de T_ϵ sont donc toutes différentes, la matrice T_ϵ est donc diagonalisable. On en déduit que $PT_\epsilon P^{-1}$ est également diagonalisable et de plus elle tend vers A, ce qui montre la densité des matrices diagonalisables.

3)

a) Le problème vient du fait qu'il ne semble pas possible d'approcher une matrice qui aurait des valeurs propres complexes conjuguées par une matrice dont les valeurs propres sont réelles. On considère le cas de la dimension 2. Soit $\phi : M_2(\mathbb{R}) \to \mathbb{R}$ qui a M associe le discriminant de son polynôme caractéristique. L'application ϕ est continue et pour A diagonalisable, on a $\phi(A) \geq 0$. Or pour B dont les valeurs propres sont complexes conjuguées, on a $\phi(B) < 0$. Par continuité de ϕ, il n'est donc pas possible d'approcher B par des matrices diagonalisables.

b) Si $|Im(z)|^n \leq |P(z)|, \forall z \in \mathbb{C}$ alors en particulier une racine de P vérifie $Im(z) = 0$ et donc elle est réelle, ce qui montre que P est scindé sur $\mathbb{R}$. Dans l'autre sens, si P est scindé sur $\mathbb{R}$, on a en notant x_k ses racines (avec répétition) :

$$|P(z)|^2 = \prod_{k=1}^{n} |z - x_k|^2 = \prod_{k=1}^{n} |Re(z) - x_k + iIm(z)|^2 \geq |Im(z)|^{2n}$$

D'où le résultat.

c) Pour cela on considère A_k une suite de matrices trigonalisables qui converge vers $A \in M_n(\mathbb{R})$. On sait que A est trigonalisable si et seulement si son polynôme caractéristique est scindé sur $\mathbb{R}$ qui est équivalent à la question précédente. Donc pour tout $k \in \mathbb{N}$, on a :

$$\forall z \in \mathbb{C}, \quad |Im(z)|^n \leq |\chi_{A_k}(z)|$$

On passe alors à la limite dans l'inégalité précédente ce qui est possible par continuité du polynôme caractéristique. Ce qui montre que :

$$\forall z \in \mathbb{C}, \quad |Im(z)|^n \leq |\chi_A(z)|$$

Par équivalence on en déduit que χ_A est scindé sur $\mathbb{R}$ et donc que A est tigonalisable. D'où le résultat.

d) Si on reprend le raisonnement mené pour le cas complexe en prenant cette fois A trigonalisable, on montre alors que $\mathcal{T}_n(\mathbb{R}) \subset \overline{\mathcal{D}_n(\mathbb{R})}$ avec les notations correspondantes pour les ensembles de matrices trigonalisables et diagonalisables. Pour montrer l'inclusion contraire on a déjà $\mathcal{D}_n(\mathbb{R}) \subset \mathcal{T}_n(\mathbb{R})$ et en montrant que $\mathcal{T}_n(\mathbb{R})$ est fermé on conclut en passant à l'adhérence.

Oraux 22 : Centrale 1

1 Soient $n \in \mathbb{N}^*$ et $A \in GL_n(\mathbb{R})$.

1. Montrer que $b_A : (x, y) \mapsto (Ax|Ay)$ est un produit scalaire.
2. Montrer qu'il existe $Q \in O_n(\mathbb{R})$ et $S \in S_n(\mathbb{R})$ telles que $A = QS$. Etendre ce résultat au cas $A \in \mathcal{M}_n(\mathbb{R})$.
3. *Une suite inventée parmi les multiples applications possibles.*
   Montrer que l'ensemble des matrices de $\mathcal{M}_n(\mathbb{R})$ à déterminant > 0 est connexe par arcs.

1

1. b_A est presque immédiatement symétrique et linéaire par rapport à la première variable. De plus
$$b_A(x, x) = \|Ax\|^2 \geq 0$$
et si $b_A(x) = 0$ alors $Ax = 0$ et donc $x = 0$ car A est inversible. L'application est donc aussi positive et définie positive.
2. A^TA est une matrice symétrique et donc orthodiagonalisable. De plus, si λ est valeur propre et X vecteur propre asocié, on a
$$0 \leq \|AX\|^2 = (X|A^TAX) = \lambda\|X\|^2$$
et le spectre de A^TA est inclus dans $\mathbb{R}^+$ et même $\mathbb{R}^{+*}$ car A est inversible. En notant P une matrice orthogonale diagonalisant A^TA et $0 < \lambda_1 \leq \cdots \leq \lambda_n$ les valeurs propres, on a (quitte à permuter les colonnes de P)
$$P^{-1}A^TAP = \text{diag}(\lambda_1, \ldots, \lambda_n)$$
Les λ_i étant positifs, on peut poser
$$S = P\text{diag}(\sqrt{\lambda_1}, \ldots, \sqrt{\lambda_n})P^{-1}$$
P étant orthogonale, S est symétrique et par construction $S^2 = A^TA$. De plus, les λ_i étant non nuls, S est inversible. On pose
$$Q = AS^{-1}$$
et on a $Q^TQ = (S^{-1})^TA^TAS^{-1} = S^{-1}S^2S = I_n$ et Q est orthogonale. Par construction, $A = QS$.

   Si A n'est pas inversible, comme $GL_n(\mathbb{R})$ est dense dans $\mathcal{M}_n(\mathbb{R})$, il existe une suite (A_k) de matrices inversibles qui converge vers A.
   Pour chaque k, on trouve $Q_k$et S_k.
   (Q_k) est bornée (la norme euclidienne d'une matrice orthogonale vaut $\sqrt{n}$) et on peut (Bolzano-Weierstrass utilisable en dimension finie)en extraire une sous-suite convergente. Quitte à extraire, donc, on suppose $Q_k \to Q$ et $Q \in O_n(\mathbb{R})$ (ensemble fermé, image réciproque du fermé $\{I_n\}$ par $M \mapsto M^TM$ continue). Mais alors $S_k = Q_k^TA_k \to Q^TA = S$ et S est symétrique ($S_n(\mathbb{R})$ fermé comme sous-espace de dimension finie). On a alors $A = QS$ avec Q orthogonale et S symétrique.
3. Dans la preuve de la décomposition polaire (cas inversible), on a trouvé S à valeurs propres > 0. Notons S_n^{++} l'ensemble des matrices symétriques à spectre inclus dans $\mathbb{R}^{+*}$.
   Soient A_1, A_2 à déterminant > 0. Il existe Q_1, S_1, Q_2, S_2 telles que $A_i = Q_iS_i$ et $S_i \in S_n^{++}$.
   Comme $\det(A_i)$ et $\det(S_i)$ sont > 0, il en est de même de $\det(Q_i)$ et $Q_i \in SO_n(\mathbb{R})$.
   Si on montre que $SO_n(\mathbb{R})$ et $S_n^{++}(\mathbb{R})$ sont connexes par arcs, on pourra relier continument Q_1 et

Q_2 (application φ) et S_1 et S_2 (application ψ) en restant dans $SO_n(\mathbb{R})$ ou $S_n^{++}(\mathbb{R})$. $t \mapsto \varphi(t)\psi(t)$ sera un chemin continu de A_1 vers A_2 restant dans l'ensemble des matrices à déterminant > 0 et on pourra conclure à la connexité par arcs.

Pour $S_n^{++}(\mathbb{R})$, on se donne $S \in S_n^{++}$. Il existe $P \in O_n(\mathbb{R})$ telle que $P^{-1}SP = D$ diagonale à coefficients diagonaux > 0.
$t \mapsto P\text{diag}((1-t)d_i + t)P^{-1}$ permet de relier continument S à I_n dans S_n^{++}. Par transitivité, on a la connexité par arcs de S_n^{++}.

Pour $M \in SO_n(\mathbb{R})$, le cours indique qu'il existe P orthogonale et des réels θ_i tels que $P^{-1}MP = \text{diag}(R_{\theta_1}, \dots, R_{\theta_k}, I_q)$.
$t \mapsto P\text{diag}(R_{t\theta_1}, \dots, R_{t\theta_k}, I_q)$ permet de relier continument M et I_n dans $SO_n(\mathbb{R})$ et on conclut encore.

2 On définit

$$f : M \in \mathcal{M}_n(\mathbb{R}) \to (\text{Tr}(M), \text{Tr}(M^2), \dots, \text{Tr}(M^n))$$

On munit $\mathcal{M}_n(\mathbb{R})$ du produit scalaire $(A|B) = \text{Tr}(A^T B)$ et on note N la norme associée.

1. Montrer que $N(AB) \leq N(A)N(B)$ puis que
$$\exists \alpha,\ \forall A \in \mathcal{M}_n(\mathbb{R}),\ |\text{Tr}(A)| \leq \alpha N(A)$$
2. Montrer que f est différentiable en tout M et expliciter $df(M)$.
3. Comparer le rang de $df(M)$ au degré du polynôme minimal μ_M de M.
4. Montrer que l'ensemble $\{M \in \mathcal{M}_n(\mathbb{R}) / \ \chi_M = \mu_M\}$ est un ouvert de $\mathcal{M}_n(\mathbb{R})$.

2

1. On a
$$N(AB)^2 = \sum_{1 \leq i,j \leq n} (AB)_{i,j}^2 = \sum_{1 \leq i,j \leq n} \left(\sum_{k=1}^{n} a_{i,k} b_{k,j} \right)^2$$
Par inégalité de Cauchy-Schwarz dans $\mathbb{R}^n$,
$$N(AB)^2 \leq \sum_{1 \leq i,j \leq n} \left(\sum_{k=1}^{n} a_{i,k}^2 \right) \left(\sum_{k=1}^{n} b_{k,j}^2 \right)$$
On a ainsi
$$N(AB)^2 \leq \sum_{i=1}^{n} \left(\left(\sum_{k=1}^{n} a_{i,k}^2 \right) N(B)^2 \right) = N(A)^2 N(B)^2$$
On obtient donc la sous-multiplicativité de N.
Par inégalité de Cauchy-Schwarz, on a
$$|\text{Tr}(A)| = |(I_n|A)| \leq N(I_n)N(A) = \sqrt{n}N(A)$$
2. f est de classe C^1 car par théorème d'opération toutes ses fonctions coordonnées $f_k : M \mapsto \text{Tr}(M^k)$ le sont. De plus
$$df(M) \ : \ H \in \mathcal{M}_n(\mathbb{R}) \mapsto (df_1(M).H, \dots, df_n(M).H) \in \mathbb{R}^n$$
Pour le calcul de la différentielle de f_k en M, il ne me semble pas judicieux de revenir à des dérivées partielles et j'utilise plutôt la définition. Je forme donc
$$f_k(M+H) - f_k(M) = \text{Tr}((M+H)^k - M^k)$$

et j'essaye de l'écrire sous la forme $\varphi(H) + o(\|H\|)$. Pour cela, on développe $(M+H)^k$ et on isole les termes avec une puissance 1 pour H (attention : pas de formule du binôme puisque M et H ne commutent pas forcément) puisque les autres donneront des terme $o(\|H\|)$ (avec la sous-multiplicativité). On obtient

$$f_k(M+H) - f_k(M) = \mathrm{Tr}(M^{k-1}H + M^{k-2}HM + \cdots + MHM^{k-2} + HM^{k-1}) + o(\|H\|)$$

Par linéarité de la trace et avec la propriété $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$ on en déduit que

$$f_k(M+H) - f_k(M) = k\mathrm{Tr}(M^{k-1}H) + o(\|H\|)$$

Comme $H \mapsto k\mathrm{Tr}(M^{k-1}H)$ est linéaire, c'est la différentielle en M de f_k. Finalement,

$$df(M).H = (\mathrm{Tr}(H), 2\mathrm{Tr}(MH), \ldots, n\mathrm{Tr}(M^{n-1}H))$$

3. On a ainsi
$$\ker(df(M)) = \{H/\ \mathrm{Tr}(H) = \mathrm{Tr}(MH) = \cdots = \mathrm{Tr}(M^{n-1}H) = 0\}$$
En notant d le degré de μ_M, pour tout $k \geq d,\ M^k \in \mathrm{Vect}(I_n, \ldots, M^{d-1})$ et donc
$$\ker(df(M)) = \{H/\ \mathrm{Tr}(H) = \mathrm{Tr}(MH) = \cdots = \mathrm{Tr}(M^{d-1}H) = 0\}$$
$\ker(df(M))$ est donc l'intersection des noyaux des formes linéaires $\ell_0, \ldots, \ell_{d-1}$ où $\ell_k(H) = \mathrm{Tr}(M^kH)$. Si $\sum_{k=0}^{d-1} \alpha_k \ell_k = 0$ alors
$$\forall H,\ \mathrm{tr}\left(\sum_{k=0}^{d-1} \alpha_k M^k H\right)$$
et ceci donne $\sum_{k=0}^{d-1} \alpha_k M^k$ (utiliser pour H les $E_{i,j}$). Les formes linéaires sont indépendantes et on en tire classiquement que l'intersection des noyau est de dimension $n^2 - d$. On en déduit par théorème du rang que
$$\mathrm{rg}(df(M)) = d = \deg(\chi_d)$$

4. Par théorème de Cayley-Hamilton, $\mu_M | \chi_M$ et on a donc $\chi_M = \mu_M$ si et seulement si $\deg(\mu_M) = n$ (puisque les deux polynômes sont en outre unitaires). L'ensemble cherché est donc l'ensemble des matrices M telles que $df(M)$ est de rang n c'est à dire surjectives (puisque $df(M) \in \mathcal{L}(\mathcal{M}_n(\mathbb{R}), \mathbb{R}^n)$).
Considérons l'application ψ qui à une matrice M associe la matrice dans les bases canoniques de $df(M)$ (application continue car f est de classe C^1). $df(M)$ est de rang n si et seulement on peut trouver n colonnes indépendantes dans $\psi(M)$. Si F est une matrice à n^2 colonnes et n lignes (comme $\psi(M)$) notons alors $\Delta(F)$ la somme des carrés des déterminants des sous matrices de F obtenues en ne gardant que n colonnes. F est de rang n quand $\Delta(F) > 0$. L'ensemble cherché est donc l'image réciproque de $\mathbb{R}^{+*}$ par l'application continue $M \mapsto \Delta(\psi(M))$. C'est ainsi un ouvert.

3 Soit $n \in \mathbb{N}^*$. On note A_n l'ensemble des matrices de taille n, à coefficients dans $\mathbb{Z}$, et de déterminant égal à 1.

1. Montrer que A_n est un groupe pour la loi $\times$.
2. Montrer que
$$\forall M \in A_2, \qquad \mathrm{Tr}(M^4) = \mathrm{Tr}(M)^4 - 4\mathrm{Tr}(M)^2 + 2$$
3. En déduire que l'équation $P^4 + Q^4 = M^4$ ayant pour inconnues les matrices P, Q et M n'admet pas de solutions dans A_2.

En notant $f_k : M \to \mathrm{Tr}(M^k)$, on a, toujours en utilisant la règle de la chaine :

$$d f_k(M)(H) = d\mathrm{Tr}\left(p_k(M)\right)\left(d p_k(M)(H)\right)$$

où $p_k : M \to M^k$

Or $d\mathrm{Tr} = \mathrm{Tr}$, et :

$$(M+H)^k = M^k + \underbrace{\left(M^{k-1}H + M^{k-2}HM + \dots + HM^{k-1}\right)}_{d p_k(M)(H) \text{ linéaire et continue car dim finie}} + o(\|H\|)$$

Donc $d f_k(M)(H) = \mathrm{Tr}\left(M^{k-1}H + \dots + HM^{k-1}\right)$

Or $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$ donc finalement :

$$d f_k(M)(H) = k\,\mathrm{Tr}\left(M^{k-1}H\right).$$

et $d f(M)(H) = \left(d f_k(M)(H)\right)_{1 \le k \le n}$ ✓

2) $H \in \ker D_f(M) \iff \forall k \in [\![0; n-1]\!],\ \mathrm{Tr}\left(M^{k-1}H\right) = 0$

$\iff H^T \in \underset{0 \le i \le n-1}{\mathrm{Vect}}\left(M^i\right)^{\perp}$ ✓

3) On travaille en dimension finie, donc :

$\underbrace{\underset{0 \le i \le n-1}{\mathrm{Vect}}\left(M^i\right)^{\perp}}_{= \ker D_f(M)} \oplus \underset{0 \le i \le n-1}{\mathrm{Vect}}\left(M^i\right)$, donc par théorème

du rang, on a $\mathrm{Im}(D_f(\Pi)) \sim \underset{0 \le i \le n-1}{\mathrm{Vect}}(\Pi^i)$

et $\mathrm{rg}(D_f(\Pi)) = \dim \underset{0 \le i \le n-1}{\mathrm{Vect}}(\Pi^i)$

De plus, si $P(\Pi) \in \mathrm{Vect}(\Pi^i)$ où $P \in \mathbb{R}_{n-1}[X]$,

en faisant la div. euclidienne par μ_Π : $P = Q\mu_\Pi + R$

on a $P(\Pi) = R(\Pi)$ où $\deg R < \deg \mu_\Pi$

Réciproquement, si $\deg P < \deg \mu_\Pi$, par minimalité de μ_Π

on a $P(\Pi) \neq 0$, ce qui donne la liberté des $(\Pi^i)_{0 \le i < \deg \mu_\Pi}$

Donc $\mathrm{rg}(D_f(\Pi)) = \deg(\mu_\Pi)$. ✓

d) En notant $\varphi : \begin{cases} \mathcal{M}_n(\mathbb{R}) \to \mathbb{R} \\ \Pi \to \det D_f(\Pi) \end{cases}$, on a que

φ est continue car det et $\Pi \to D_f(\Pi)$ le sont, et alors

$\{\Pi \in \mathcal{M}_n(\mathbb{R}) \mid \deg(\mu_\Pi) = n\} = \varphi^{-1}(\underbrace{\mathbb{R}^*}_{\text{ouvert}})$ est donc ouvert ✓

Groupe multiplicatif d'un corps fini

Salim Rostam

Soit p un nombre premier. On veut montrer que $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. Plus généralement, on va montrer le résultat suivant.

Théorème 1. *Soit k un corps (commutatif). Tout sous-groupe fini de $k^\times$ est cyclique.*

Le théorème nous permettra bien de conclure puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps. On va donner deux démonstrations : la deuxième sera plus longue mais sera l'occasion de montrer quelques résultats sur $\mathbb{Z}/n\mathbb{Z}$.

Soit k un corps (commutatif). On rappelle le résultat suivant, qui nous servira pour les deux démonstrations.

Proposition 2. *Un polynôme de degré n sur k possède au plus n racines.*

Démonstration. Si $a \in k$ est une racine de $P \in k[X]$ alors par division euclidienne on peut écrire $P = (X-a)Q$ avec $\deg Q = \deg P - 1$. On recommence, et on s'arrête au plus tard quand le degré du quotient devient nul. □

Remarque 3. Cette proposition n'est plus valable si k n'est pas commutatif ! Par exemple, le polynôme X^2+1 possède une infinité de racines dans le corps (non commutatif, donc) des *quaternions*.

1 Première preuve

On rappelle tout d'abord les résultats suivants.

Lemme 4. *Soit G un groupe et soit $g \in G$ un élément d'ordre fini n. Alors pour tout $a \in \mathbb{N}^*$, l'élément g^a est d'ordre $\frac{n}{\mathrm{pgcd}(n,a)}$. En particulier, si n et a sont premiers entre eux alors g^a est d'ordre n.*

Démonstration. Tout d'abord, remarquons que l'ordre de g^a divise n puisque $(g^a)^n = g^{an} = (g^n)^a = 1^a = 1$. L'ordre de g^a est donné par le plus petit $\omega \in \{1, \dots, n\}$ tel que $(g^a)^\omega = 1$. On a $g^{a\omega} = 1$ donc $n \mid a\omega$, donc il existe $k \in \mathbb{N}^*$ tel que $a\omega = kn$. Écrivons $n = \mathrm{pgcd}(n,a)n'$ et $a = \mathrm{pgcd}(n,a)a'$, avec donc n' et a' premiers entre eux. On obtient $a'\omega = kn'$, donc n' divise ω. Le plus petit ω possible est donc $n' = \frac{n}{\mathrm{pgcd}(n,a)}$. □

Lemme 5. *Soit G un groupe et soit g (resp. h) un élément d'ordre fini a (resp. b) de G. Si g et h commutent et si a et b sont premiers entre eux, alors gh est d'ordre ab.*

Démonstration. Puisque g et h commutent on a $(gh)^{ab} = (g^a)^b(h^b)^a = 1$ donc l'ordre de gh divise ab. Mais si $(gh)^k = 1$ alors $g^k = h^{-k}$ est un élément dont l'ordre divise a et b donc divise $\mathrm{pgcd}(a,b) = 1$, donc $g^k = h^{-k} = 1$ donc a et b divisent k donc ab divise k (puisque a et b sont premiers entre eux). □

Remarque 6. Les deux hypothèses sont essentielles !

— Si les éléments ne commutent pas c'est la catastrophe car gh peut devenir d'ordre infini. Par exemple, on peut considérer le groupe $\langle a, b : a^2 = b^2 = 1\rangle$, ou bien, pour ceux qui n'aiment pas les groupes définis par générateurs et relations, on peut considérer le sous-groupe des isométries de $\mathbb{R}^2$ engendré par les symétries orthogonales d'axe $x = 0$ et $x = 1$. Si on veut rester dans un groupe fini, on peut par exemple considérer les deux matrices $g := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ et $h := \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ d'ordre 2 de $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, dont le produit $gh = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ est d'ordre 3.
— Si les éléments commutent mais que les ordres ne sont pas premiers entre eux, on peut par exemple prendre $h := g^k$. Par le Lemme 4, l'élément h est d'ordre $\frac{a}{\mathrm{pgcd}(a,k)}$ et $gh = g^{k+1}$ est d'ordre $\frac{a}{\mathrm{pgcd}(a,k+1)}$, qui n'a aucune raison d'être égal à $a\frac{a}{\mathrm{pgcd}(a,k)}$ (si vous n'êtes pas convaincus, prenez $h = g^{-1}$!).

(Je ne trouve plus la référence bibliographique pour la suite de la preuve, si vous en avez une n'hésitez pas à me l'indiquer.) Soit H un sous-groupe fini non trivial de $k^\times$. Notons $n := |H|$ et écrivons $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ la décomposition de n en produit de facteurs premiers. Par le Lemme 5, il suffit de montrer que H possède un élément d'ordre $p_i^{\alpha_i}$ pour chaque i.

S'il existe $x \in H$ d'ordre $p_i^{\alpha_i} q$ avec $q := \prod_{j\neq i} p_i^{\beta_j}$ et $0 \leq \beta_j \leq \alpha_i$, alors par le Lemme 4 l'élément x^q est d'ordre $p_i^{\alpha_i}$ et c'est gagné. On va montrer que l'on est nécessairement dans ce cas. Si chaque $x \in H$ est d'ordre $p_i^{\beta_i} q$ où $q := \prod_{j\neq i} p_j^{\beta_j}$ avec $\beta_i < \alpha_i$ et $0 \leq \beta_j \leq \alpha_j$ si $j \neq i$, alors x est d'ordre divisant $p_i^{\alpha_i - 1} q = \frac{n}{p_i}$. Ainsi, les éléments de H sont des racines de $X^{\frac{n}{p_i}} - 1$, mais alors par la Proposition 2 on aurait $|H| \leq \frac{n}{p_i}$ ce qui est absurde.

2 Deuxième preuve

Cette preuve est plus longue mais sera l'occasion d'énoncer quelques résultats complémentaires.

2.1 Indicatrice d'Euler

Définition 7. Si $n \in \mathbb{N}^*$, on note $\varphi(n)$ le nombre d'éléments de $\{1, \ldots, n\}$ premiers avec n. La fonction $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ est appelée *indicatrice d'Euler*.

Énonçons quelques propriétés élémentaires de la fonction φ.

Propriété 8. *Si p est premier alors $\varphi(p) = p - 1$.*

Démonstration. En effet, chaque élément de $\{1, \ldots, p-1\}$ est premier à p. □

Propriété 9. *Si $n \in \mathbb{N}^*$ on a $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$.*

Démonstration. Vient du fait que $k \in \{1, \ldots, n\}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si k est premier à n. □

Proposition 10. *Soit $n \in \mathbb{N}^*$. On a $n = \sum_{d|n} \varphi(n)$.*

Démonstration. (Voir [Gou, Proposition 6 page 32].) On écrit les fractions $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}$ sous forme irréductible. On obtient chaque $\frac{k}{d}$, où $d \mid n$ et $k \in \{1, \ldots, d\}$ est premier à d. Ainsi, pour chaque $d \mid n$ il y a exactement $\varphi(d)$ fractions avec d au dénominateur. Au départ on avait n fractions, on conclut donc que $n = \sum_{d|n} \varphi(d)$. □

On peut également déduire cette proposition du lemme suivant.