LUNDI 18 MAI

Référence	Origine	Thèmes
136-549	Mines MP	Groupes, réduction des endomorphismes
136-771	"	Exponentielle de matrices
136-794	"	Calcul différentiel, applications linéaires
136-798	"	Calcul différentiel, espaces euclidiens
136-807	"	Probabilités
136-813	"	Probabilités
136-1179	Centrale MP	Algèbre linéaire
136-1388	Mines Telecom MP	Espaces euclidiens
135-490	Mines MP	Groupes

NB : L'exercice **136-1388** tel qu'il est posé dans la RMS n'est clairement pas un exercice pour le concours Mines Telecom ! En revanche, l'énoncé qui figure dans ce corrigé est du niveau Mines Telecom.

rms136-549

Soit H*, un sous-groupe fini de* $GL_n(\mathbb{R})$*. On suppose que*

$$\forall f \in H, \qquad Sp_{\mathbb{C}}(f) \subset \{-1;\ 1\}.$$

[**1.**] *Démontrer que* H *est commutatif.*
[**2.**] *Déterminer les valeurs possibles du cardinal de* H*.*

[**1.**] Soit $f \in H$.

Le polynôme caractéristique est scindé dans $\mathbb{C}[X]$ (comme tout polynôme de degré $n \geqslant 1$ à coefficients réels) et, par hypothèse, ses racines sont réelles, donc il est en fait scindé dans $\mathbb{R}[X]$. Par conséquent, f est trigonalisable.

❧ Si f est diagonalisable, alors son polynôme minimal est scindé à racines simples et les racines de son polynôme minimal sont les valeurs propres de f. Dans ces conditions, le polynôme

$$(X-1)(X+1)$$

est un polynôme annulateur de f et $f^2 = I_{\mathbb{R}^n}$.

❧

Comme $f \in H$ et que H est un groupe, on sait que $f^k \in H$ pour tout $k \in \mathbb{N}$. Mais comme H est un groupe **finie**, l'élément f est d'ordre fini et il existe donc un entier $d \geqslant 1$ tel que $f^d = I_{\mathbb{R}^n}$.

Comme $d = \ell - k \geqslant 1$, le polynôme annulateur $X^d - 1$ est scindé à racines simples. Le polynôme minimal de f divise ce polynôme annulateur, donc il est lui aussi scindé à racines simples (en tant que polynôme à coefficients complexes).

Et comme on sait que les valeurs propres de f appartiennent à $\{\pm 1\}$, on en déduit que

$$(X-1)(X+1)$$

est un polynôme annulateur de f. Finalement, f est nécessairement diagonalisable !

❧ Sachant que $f^2 = I_{\mathbb{R}^n}$ pour tout $f \in H$, on sait que H est commutatif, cf **[rms135-490]**.

[**2.**] Le cardinal de H est une puissance de 2, cf **[rms135-490]**.

rms136-771

*Une matrice $M \in \mathfrak{M}_n(\mathbb{R})$ est dite **stochastique** lorsque tous ses coefficients sont positifs et que la somme des coefficients de chaque ligne est égale à 1.*
Déterminer les matrices $A \in \mathfrak{M}_n(\mathbb{R})$ telle que, pour tout $t \in \mathbb{R}_+$, la matrice $\exp(tA)$ soit stochastique.

On note $J \in \mathfrak{M}_{n,1}(\mathbb{R})$, le vecteur colonne dont tous les coefficients sont égaux à 1.

❧ Les coefficients du vecteur colonne MJ sont les sommes des coefficients de M calculées ligne par ligne. Il faut donc que

$$\forall\, t \in \mathbb{R}_+, \qquad \exp(tA).J = J.$$

La fonction $t \mapsto \exp(tA)$ est dérivable sur $\mathbb{R}$ et sa dérivée en $t = 0$ est égale à A. L'application $M \mapsto M.J$ étant linéaire sur un espace de dimension finie, on en déduit que l'application $t \mapsto \exp(tA).J$ est dérivable sur $\mathbb{R}$ et que sa dérivée en 0 est égale à $A.J$. Comme cette application est constante, on en déduit que

$$A.J = 0_{n,1}. \tag{$\star$}$$

❧ Par ailleurs, On connaît le développement limité de $\exp(tA)$ au voisinage de $t = 0$:

$$\exp(tA) \underset{t\to 0}{=} I_n + tA + o(t).$$

Comme les coefficients de $\exp(tA)$ sont tous positifs, on en déduit en particulier que les coefficients non diagonaux de tA sont tous positifs pour t assez petit. Il faut donc également que

$$\forall\, 1 \leqslant i \neq j \leqslant n, \qquad a_{i,j} \geqslant 0. \tag{$\dagger$}$$

✍ *Comme la somme des coefficients de chaque ligne de A est nulle, il faut donc que tous les coefficients diagonaux soient négatifs.*

❧ Réciproquement, considérons une matrice A qui vérifie les deux conditions $(\star)$ et $(\dagger)$.
Une récurrence évidente montre que $A^k J = 0$ pour tout $k \in \mathbb{N}^*$ et l'application $P \mapsto PJ$ étant continue, on en déduit que

$$\forall\, t \in \mathbb{R}_+, \qquad \exp(tA)J = \sum_{k=0}^{+\infty} \frac{1}{k!} A^k J = I_n J = J.$$

La condition sur les lignes de $\exp(tA)J$ est donc vérifiée.
Soit $\lambda_0 \in \mathbb{R}_-$, le plus petit coefficient diagonal de A. (Il n'y a qu'un nombre fini de coefficients diagonaux !) L'astuce taupinale nous donne

$$A = \lambda_0 I_n + (A - \lambda_0 I_n)$$

et, par définition de λ_0, tous les coefficients de la matrice $B = (A - \lambda_0 I_n)$ sont positifs. Comme $\lambda_0 I_n$ et B commutent, on sait que

$$\forall\, t \in \mathbb{R}_+, \qquad \exp(tA) = \exp(t\lambda_0 I_n)\exp(tB) = e^{\lambda_0 t}\exp(tB).$$

Le facteur $e^{\lambda_0 t}$ est évidemment positif. Comme tous les coefficients de B sont positifs, alors tous les coefficients de B^k sont positifs, quel que soit $k \in \mathbb{N}$ (formule du produit matriciel), donc tous les coefficients de $\exp(tB)$ sont positifs et finalement tous les coefficients de $\exp(tA)$ sont positifs.

❧ Une condition nécessaire et suffisante pour que la matrice $\exp(tA)$ soit stochastique pour tout $t \in \mathbb{R}_+$ est que $AJ = J$ et que tous les coefficients non diagonaux de A soient positifs.

✍ *Dans la théorie des chaînes de Markov à espace d'états finis, la matrice A est appelée le **générateur infinitésimal** de la matrice de transition (=la matrice qui exprime la loi conditionnelle de X_t sachant la loi de X_0).*

rms136-794

On considère l'application $f : \mathfrak{M}_n(\mathbb{R}) \to \mathcal{S}_n(\mathbb{R})$ *définie par*

$$\forall\, P \in \mathfrak{M}_n(\mathbb{R}), \qquad f(P) = P^\top.P.$$

[**1.**] *On suppose que* $M \in \mathrm{GL}_n(\mathbb{R})$. *Démontrer que la différentielle de* f *en* M *est surjective.*
[**2.**] *On note* g, *la restriction de* f *à* $\mathcal{S}_n(\mathbb{R})$ *et on considère* $M \in \mathcal{S}_n(\mathbb{R}) \cap \mathrm{GL}_n(\mathbb{R})$. *La différentielle de* g *en* M *est-elle surjective ?*

[**1.**] Tout d'abord, le produit $P^\top.P$ est bien une matrice symétrique réelle, quelle que soit la matrice $P \in \mathfrak{M}_n(\mathbb{R})$.

Ensuite, f est de classe $\mathscr{C}^\infty$ sur $\mathfrak{M}_n(\mathbb{R})$ comme produit de deux applications linéaires.

Enfin, le développement de l'expression

$$f(M+H) = f(M) + \big(M^\top.H + H^\top.M\big) + f(H)$$

fait apparaître

— une application linéaire : $H \mapsto M^\top.H + H^\top.M$

— un reste sous-linéaire : pour une norme sous-multiplicative sur $\mathfrak{M}_n(\mathbb{R})$,

$$\|H^\top.H\| \leqslant \|H^\top\|\|H\| \leqslant K\|H\|^2$$

où K est une constante de Lipschitz pour la transposition (application linéaire continue, quelle que soit la norme $\|\cdot\|$ choisie).

Par identification,

$$\forall\, M \in \mathfrak{M}_n(\mathbb{R}), \qquad df(M) = \big[H \mapsto M^\top.H + H^\top.M\big].$$

❧ Par construction, l'application $df(M)$ est à valeurs dans $\mathcal{S}_n(\mathbb{R})$ (= l'espace d'arrivée de f). En fait,

$$H^\top.M = (M^\top.H)^\top.$$

Par conséquent,

$$\begin{aligned} H \in \mathrm{Ker}\ df(M) &\iff (M^\top.H) + (M^\top.H)^\top = 0_n \\ &\iff (M^\top.H)^\top = -(M^\top.H) \end{aligned}$$

et comme la matrice M est ici supposée inversible, on en déduit que

$$H \in \mathrm{Ker}\ df(M) \iff \exists\, A \in \mathfrak{A}_n(\mathbb{R}), \quad H = (M^\top)^{-1}.A.$$

L'application $Q \mapsto (M^\top)^{-1}.Q$ réalise un isomorphisme de l'espace $\mathfrak{A}_n(\mathbb{R})$ des matrices antisymétriques réelles sur $\mathrm{Ker}\ df(M)$, donc

$$\dim \mathrm{Ker}\ df(M) = \dim \mathfrak{A}_n(\mathbb{R}).$$

On sait que $\mathcal{S}_n(\mathbb{R})$ et $\mathfrak{A}_n(\mathbb{R})$ sont supplémentaires dans $\mathfrak{M}_n(\mathbb{R})$. On déduit alors du Théorème du rang que

$$\mathrm{rg}\ df(M) = \dim \mathfrak{M}_n(\mathbb{R}) - \dim \mathfrak{A}_n(\mathbb{R}) = \dim \mathcal{S}_n(\mathbb{R})$$

et comme on a remarqué que $\mathrm{Im}\ df(M) \subset \mathcal{S}_n(\mathbb{R})$, on peut conclure :

$$\mathrm{Im}\ df(M) = \mathcal{S}_n(\mathbb{R})$$

donc $df(M)$ est sujective.

[**2.**] Les calculs sont les mêmes, la seule différence tient à l'espace de départ : l'application linéaire $dg(M)$ est cette fois-ci un endomorphisme de $\mathcal{S}_n(\mathbb{R})$.

Le raisonnement précédent montre que $dg(M)$ est injective (la seule matrice à la fois symétrique et antisymétrique est la matrice nulle) et le Théorème du rang nous mène à la même conclusion : si la matrice M est inversible, alors l'application linéaire tangente $dg(M)$ est surjective.

✍ *La question de la surjectivité de* $dg(M)$ *paraît anecdotique dans le cadre du programme mais en fait il n'en est rien : cette propriété permet de déterminer facilement l'ensemble des vecteurs tangents à la "surface" d'équation* $[f(M) = Cte]$ *au moyen du Théorème des fonctions implicites.*

rms136-798

Soit $n \geqslant 2$. On considère une application $f : \mathbb{R}^n \to \mathbb{R}$ de classe $\mathscr{C}^2$ telle que, pour tout $x \in \mathbb{R}^n$, les valeurs propres de la hessienne de f au point x soient toutes supérieures à 1.

[**1.**] *Démontrer que*

$$\forall\, x \in \mathbb{R}^n, \qquad f(x) \geqslant f(0) + \big\langle\, \nabla f(x) \,\big|\, x \,\big\rangle + \frac{\|x\|^2}{2}.$$

[**2.**] *En déduire que f atteint un minimum global.*

[**1.**] Pour comparer la valeur $f(x)$ à la valeur $f(0)$, on paramètre le segment $[0, x]$ et on considère donc l'application $g : \mathbb{R} \to \mathbb{R}$ définie par

$$\forall\, t \in \mathbb{R}, \qquad g(t) = f(t \cdot x).$$

Par composition de fonctions, la fonction g est de classe $\mathscr{C}^2$ sur $\mathbb{R}$ et, d'après la règle de la chaîne,

$$\begin{aligned}
\forall\, t \in \mathbb{R}, \qquad g'(t) &= df(t \cdot x)(x) = \sum_{k=1}^{n} \frac{\partial f}{\partial x_k}(t \cdot x) \cdot x_k \\
g''(t) &= \sum_{k=1}^{n} x_k \cdot \Big(\sum_{\ell=1}^{n} \frac{\partial}{\partial x_\ell} \frac{\partial f}{\partial x_k}(t \cdot x) \Big) \\
&= \sum_{k=1}^{n} \sum_{\ell=1}^{n} x_k \frac{\partial^2 f}{\partial x_k \partial x_\ell}(t \cdot x) x_\ell \\
&= x^\top . H_f(t \cdot x) . x.
\end{aligned}$$

❧ Soit $S \in \mathfrak{M}_n(\mathbb{R})$, une matrice symétrique réelle. D'après le Théorème spectral, pour tout $x \in \mathbb{R}^n$, il existe une famille orthogonale $(x_\lambda)_{\lambda \in \mathrm{Sp}(S)}$ telle que

$$x = \sum_{\lambda \in \mathrm{Sp}(S)} x_\lambda \qquad \text{et} \qquad \forall\, \lambda \in \mathrm{Sp}(S), \quad S x_\lambda = \lambda x_\lambda.$$

On en déduit (Théorème de Pythagore) que

$$\big\langle\, x \,\big|\, Sx \,\big\rangle = \sum_{\lambda \in \mathrm{Sp}(S)} \lambda \|x_\lambda\|^2 \geqslant \min\big[\mathrm{Sp}(S)\big] \sum_{\lambda \in \mathrm{Sp}(S)} \|x_\lambda\|^2 = \min\big[\mathrm{Sp}(S)\big]\, \|x\|^2.$$

La matrice hessienne $H_f(t \cdot x)$ est symétrique réelle (Théorème de Schwarz, la fonction f est de classe $\mathscr{C}^2$) et ses valeurs propres sont toutes supérieures à 1, donc

$$\forall\, x \in \mathbb{R}^n,\ \forall\, t \in [0,1], \qquad x^\top . H_f(t \cdot x) . x \geqslant \|x\|^2.$$

❧ La fonction g étant de classe $\mathscr{C}^2$ sur $\mathbb{R}$, on déduit de la formule de Taylor avec reste intégral que

$$g(1) = g(0) + g'(0) \cdot (1 - 0) + \int_0^1 g''(t) \frac{(1-t)^1}{1!}\, dt$$

et donc que

$$f(x) = f(0) + \big\langle\, \nabla f(0) \,\big|\, x \,\big\rangle + \int_0^1 \big[x^\top . H_f(t \cdot x) . x\big](1-t)\, dt.$$

D'après ce qui précède,

$$\forall\, t \in [0,1], \quad \big[x^\top . H_f(t \cdot x) . x\big] \underbrace{(1-t)}_{\geqslant 0} \geqslant \|x\|^2 (1-t)$$

donc

$$\int_0^1 \big[x^\top . H_f(t \cdot x) . x\big](1-t)\, dt \geqslant \int_0^1 \|x\|^2 (1-t)\, dt = \frac{\|x\|^2}{2}.$$

La minoration demandée est ainsi démontrée.

[**2.**] D'après l'inégalité de Schwarz,

$$\forall\, x \in \mathbb{R}^n, \qquad \left|\left\langle \nabla f(0) \,\middle|\, x \right\rangle\right| \leqslant \left\|\nabla f(0)\right\| \|x\|.$$

Par croissances comparées de $\|x\|$ et de $\|x\|^2$,

$$\lim_{\|x\|\to+\infty} f(0) + \left\langle \nabla f(x) \,\middle|\, x \right\rangle + \frac{\|x\|^2}{2} = +\infty,$$

donc f tend vers $+\infty$ au voisinage de l'infini.

❧ Soit $A > f(0)$. Il existe donc $R > 0$ tel que

$$\forall\, x \in \mathbb{R}^n, \qquad \|x\| > R \implies f(x) \geqslant A.$$

La boule fermée $[\|x\| \leqslant R]$ est compacte (fermée et bornée dans un espace vectoriel de dimension finie) et f est continue sur $\mathbb{R}^n$, donc (Théorème des bornes atteintes), il existe un point x_0 tel que

$$\|x_0\| \leqslant R \qquad \text{et} \qquad \forall\, x \in \mathbb{R}^n, \quad \|x\| \leqslant R \implies f(x) \geqslant f(x_0).$$

En particulier, $f(0) \geqslant f(x_0)$ et donc $A > f(x_0)$.

Par définition de R,

$$\forall\, x \in \mathbb{R}^n, \qquad \|x\| > R \implies f(x) \geqslant A,$$

on en déduit que

$$\forall\, x \in \mathbb{R}^n, \qquad f(x) \geqslant f(x_0).$$

La valeur $f(x_0)$ est donc le minimum de f sur $\mathbb{R}^n$.

✍ *Comme f est de classe $\mathscr{C}^1$ et atteint une valeur extrémale en x_0, on sait que $\nabla f(x_0) = 0$. Un raisonnement analogue à celui qu'on a fait dans la première question montre alors que*

$$\forall\, x \in \mathbb{R}^n, \qquad f(x) \geqslant f(x_0) + \left\langle \nabla f(x_0) \,\middle|\, x - x_0 \right\rangle + \frac{\|x - x_0\|^2}{2} = f(x_0) + \frac{\|x - x_0\|^2}{2}.$$

Par conséquent, la fonction f atteint un minimum local strict au point x_0.

Soit $n \geqslant 2$. On considère deux variables aléatoires X et Y, définies sur un même espace probabilisé $(\Omega, \mathcal{A}, \mathbf{P})$, indépendantes, qui suivent la loi uniforme sur l'ensemble $\mathfrak{P}([\![1,n]\!])$.
[1.] Déterminer $\mathbf{E}[\#(X)]$.
[2.] Déterminer $\mathbf{E}[\#(X \cap Y)]$.

[1.] On peut répondre naïvement à cette première question.
La fonction $C : \Omega \to \mathbb{N}$ définie par

$$\forall\, \omega \in \Omega, \qquad C(\omega) = \#\big(X(\omega)\big)$$

est une variable aléatoire discrète.

✍ *Toute fonction d'une variable aléatoire discrète est encore une variable aléatoire discrète.*

Le cardinal d'une partie E de $[\![1,n]\!]$ est un entier compris entre 0 (partie vide) et n (cas de l'intervalle $[\![1,n]\!]$ lui-même) et, pour tout entier $0 \leqslant k \leqslant n$, il existe $\binom{n}{k}$ parties de cardinal k dans $[\![1,n]\!]$ (par définition des coefficients binomiaux).
Comme X suit la loi uniforme sur l'ensemble fini $\mathfrak{P}([\![1,n]\!])$ dont le cardinal est égal à 2^n, on en déduit que

$$\forall\, 0 \leqslant k \leqslant n, \qquad \mathbf{P}(C = k) = \binom{n}{k} \cdot \frac{1}{2^n}.$$

Autrement dit, la variable aléatoire C suit la loi binomiale $\mathscr{B}(n, 1/2)$ et son espérance est donc égale à $n/2$.
❧ On peut aussi proposer une réponse moins naïve, qui permettra de répondre également à la seconde question.
Pour $1 \leqslant k \leqslant n$, on définit l'application

$$\pi_k : \mathfrak{P}\big([\![1,n]\!]\big) \to \{0;1\}$$

par

$$\forall\, E \subset [\![1,n]\!], \qquad \pi_k(E) = \mathbb{1}_{k \in E}.$$

Il est alors clair que les fonctions $\pi_1(X), \dots, \pi_n(X)$ sont des variables aléatoires de Bernoulli.
Pour $1 \leqslant k \leqslant n$, l'application $[E \mapsto E \cup \{k\}]$ réalise une bijection de l'ensemble des parties de $[\![1,n]\!]$ qui ne contiennent pas k sur l'ensemble des parties de $[\![1,n]\!]$ qui contiennent k.

✍ *La bijection réciproque est l'application $[E \mapsto E \setminus \{k\}]$.*

Par conséquent, il existe 2^{n-1} parties de $[\![1,n]\!]$ qui contiennent k et 2^{n-1} parties qui ne contiennent pas k. Comme X suit la loi uniforme sur $\mathfrak{P}([\![1,n]\!])$, on en déduit que

$$\mathbf{P}\big(\pi_k(X) = 1\big) = \mathbf{P}\big(\pi_k(X) = 0\big) = \frac{2^{n-1}}{2^n} = \frac{1}{2}.$$

Les variables aléatoires $\pi_k(X)$ suivent donc toutes la loi de Bernoulli $\mathscr{B}(1/2)$.
Enfin, la connaissance des valeurs de $\pi_1(X(\omega)), \dots, \pi_n(X(\omega))$ déterminent l'ensemble $X(\omega)$:

$$\forall\, k \in [\![1,n]\!], \qquad k \in X(\omega) \iff \pi_k\big(X(\omega)\big) = 1.$$

Donc

$$\forall\, (\varepsilon_1, \dots, \varepsilon_n) \in \{0;1\}^n, \qquad \mathbf{P}\big(\pi_1(X) = \varepsilon_1, \dots, \pi_n(X) = \varepsilon_n\big) = \mathbf{P}\big(X = \{1 \leqslant k \leqslant n \,:\, \varepsilon_k = 1\}\big) = \frac{1}{2^n}.$$

On a ainsi démontré que

$$\forall\, (\varepsilon_1, \dots, \varepsilon_n) \in \{0;1\}^n, \qquad \mathbf{P}\big(\pi_1(X) = \varepsilon_1, \dots, \pi_n(X) = \varepsilon_n\big) = \prod_{k=1}^{n} \mathbf{P}\big(\pi_k(X) = \varepsilon_k\big)$$

et donc que $(\pi_1(X), \dots, \pi_n(X))$ est une famille de variables aléatoires indépendantes.

✍ *En quelque sorte, la variable aléatoire de Bernoulli $\pi_k(X)$ "compte" si l'entier k appartient à la partie aléatoire X.*

La variable aléatoire C peut aussi s'exprimer sous la forme

$$C = \sum_{k=1}^{n} \pi_k(X)$$

et suit donc la loi binomiale $\mathscr{B}(n, 1/2)$ en tant que somme de n variables aléatoires indépendantes qui suivent toutes la loi de Bernoulli $\mathscr{B}(1/2)$.

[**2.**] Comme X et Y sont des variables aléatoires indépendantes qui suivent la loi uniforme sur $[\![1, n]\!]$, les variables aléatoires

$$\pi_1(X), \dots, \pi_n(X), \pi_1(Y), \dots, \pi_n(Y)$$

sont indépendantes et suivent toutes la loi de Bernoulli $\mathscr{B}(1/2)$.

Pour $1 \leqslant k \leqslant n$, l'entier k appartient à $X(\omega) \cap Y(\omega)$ si, et seulement si,

$$\pi_k(X(\omega)) = \pi_k(Y(\omega)) = 1,$$

c'est-à-dire si le produit $\pi_k(X(\omega))\pi_k(Y(\omega))$ est égal à 1.

Par conséquent, les variables aléatoires

$$\pi_1(X)\pi_1(Y), \dots, \pi_n(X)\pi_n(Y)$$

sont indépendantes (lemme des coalitions) et suivent toutes la loi de Bernoulli de paramètre

$$\mathbf{P}\big(\pi_k(X)\pi_k(Y) = 1\big) = \mathbf{P}\big(\pi_k(X) = 1, \pi_k(Y) = 1\big) = \frac{1}{4}.$$

On en déduit que

$$\forall\, \omega \in \Omega, \qquad \#\big(X(\omega) \cap Y(\omega)\big) = \sum_{k=1}^{n} \pi_k\big(X(\omega)\big)\pi_k\big(Y(\omega)\big)$$

et donc que le cardinal de $X \cap Y$ suit la loi binomiale $\mathscr{B}(n, 1/4)$.

Donc

$$\mathbf{E}[\#(X \cap Y)] = \frac{n}{4}.$$

Pour $k \in \mathbb{N}^*$, on pose

$$\mathbf{P}(X = k) = \frac{k-1}{2^k}.$$

[1.] *Démontrer que cette relation définit une loi de probabilité.*
[2.] *Calculer la fonction génératrice de X.*
[3.] *Calculer l'espérance de X.*

[1.] **Version élémentaire.**

Une famille $(p_k)_{k\in\mathbb{N}^*}$ est une loi de probabilité si, et seulement si, c'est une famille *sommable* de réels *positifs* dont la somme est *égale à* 1.

Il est clair que la famille considérée est une famille de réels positifs et qu'elle est sommable (règle de d'Alembert).

Le rayon de convergence de la série entière $\sum x^k$ est égal à 1, donc

$$\forall\, x \in]-1,1[, \qquad \sum_{k=1}^{+\infty} \frac{k}{x} x^{k-1} = \frac{d}{dx}\Big(\sum_{k=0}^{+\infty} x^k\Big) = \frac{1}{(1-x)^2}.$$

On en déduit que

$$\forall\, x \in]-1,1[, \qquad \sum_{k=1}^{+\infty} k x^{k+1} = \frac{x^2}{(1-x)^2}. \tag{$\star$}$$

En particulier, pour $x = 1/2$,

$$\begin{aligned}
\sum_{k=1}^{+\infty} \frac{k-1}{2^k} &= \sum_{k=0}^{+\infty} \frac{k}{2^{k+1}} && \text{(changement d'indice)}\\
&= \sum_{k=1}^{+\infty} \frac{k}{2^{k+1}} && \text{(premier terme nul)}\\
&= 1.
\end{aligned}$$

Donc on a bien défini une loi de probabilité.

Version savante.

Pour $k \in \mathbb{N}^*$, on pose $g_k = (1/2)^k$: on reconnaît la loi géométrique $\mathscr{G}(1/2)$. On "complète" en posant en outre $g_0 = 0$ (ce sera plus simple).

Le produit de Cauchy donne alors la loi de la somme de deux variables aléatoires indépendantes qui suivent toutes les deux la loi $\mathscr{G}(1/2)$ et ce produit de Cauchy est défini par

$$\begin{aligned}
\forall\, n \in \mathbb{N}, \qquad c_n &= \sum_{k=0}^{n} g_k g_{n-k}\\
&= \sum_{k=1}^{n-1} g_k g_{n-k} && \text{(car } g_0 = g_{n-n} = 0\text{)}\\
&= (n-1)2^{-n}. && \text{(tous les termes sont égaux)}
\end{aligned}$$

Donc la famille $\big((n-1)2^{-n}\big)_{n\geqslant 2}$ est bien une loi de probabilité.

[2.] Par définition,

$$\forall\, t \in [0,1], \qquad G_X(t) = \sum_{k=2}^{+\infty} (k-1)\frac{t^k}{2^k} = \sum_{k=2}^{+\infty} (k-1)(t/2)^{k-1}.$$

D'après $(\star)$,

$$\forall\, t \in [0,1], \qquad G_X(t) = \Big(\frac{t}{2-t}\Big)^2.$$

✍ *On sait que la fonction génératrice de la loi $\mathscr{G}(p)$ est définie par*

$$\forall\, t \in [0,1], \qquad F(t) = \frac{pt}{1-qt}.$$

Ayant remarqué que X était la somme de deux variables aléatoires indépendantes *et de même loi, on en déduit que*

$$\forall\, t \in [0,1], \qquad G_X(t) = \big[F(t)\big]^2$$

avec $p = q = 1/2$.

[**3.**] La fonction génératrice G_X est la somme d'une série entière dont le rayon de convergence est égal à 2, donc elle est dérivable en $t = 1$. Par conséquent,

$$\mathbf{E}(X) = G'_X(1).$$

✍ *Il faut remarquer qu'on dérive le carré d'une* ***homographie****, on peut ainsi se simplifier la tâche.*

Pour tout $t \in [0,1]$,

$$\frac{t}{2-t} = -1 + \frac{2}{2-t}$$

donc

$$G'_X(t) = 2 \cdot \frac{t}{2-t} \cdot \frac{2}{(2-t)^2} = \frac{4t}{(2-t)^3}$$

et en particulier $\mathbf{E}(X) = 4$.

✍ *On sait que l'espérance d'une variable aléatoire de loi $\mathscr{G}(p)$ est égale à $1/p$. Par linéarité de l'espérance,* $\mathbf{E}(X) = 2 \cdot 2 = 4$.

rms136-1179

Dans ce qui suit, $\mathbb{K}$ désigne un corps.
[Question de cours]
Énoncer le Théorème de la division euclidienne dans $\mathbb{K}[X]$.
[Question de cours]
Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Déterminer le reste de la division euclidienne de P par $(X-a)^2$. En déduire une condition nécessaire et suffisante pour que a soit racine simple de P.
[**1.**] *Soit $n \geqslant 2$. On pose*

$$P_n = X^n - X + (-1)^n.$$

Déterminer le nombre de racines de P_n dans $\mathbb{Q}$, dans $\mathbb{R}$ et dans $\mathbb{C}$.
[**2.**] *On note $a_1, \dots, a_n$, les racines complexes de P_n (comptées avec multiplicité). Calculer le déterminant de la matrice*

$$M = \begin{pmatrix} 1+a_1 & 1 & \cdots & 1 \\ 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \cdots & 1 & 1+a_n \end{pmatrix}.$$

[**1.**] Si $x = p/q$ est une racine rationnelle de P_n (écrite sous forme irréductible), alors

$$p^n - pq^{n-1} + (-1)^n q^n = 0$$

donc $p^n = q^{n-1}[p - (-1)^n q]$. Par conséquent, l'entier q divise p^n alors que, par hypothèse, p et q sont premiers entre eux. On en déduit que $q = 1$ et donc que $p^n - p + (-1)^n = 0$, c'est-à-dire

$$p(p^{n-1} - 1) = (-1)^{n+1}.$$

Donc p divise (-1) et par conséquent $x = \pm 1$.
Or $P_n(1) = (-1)^n \neq 0$ et $P_n(-1) = 2.(-1)^n + 1 \neq 0$. Donc P_n n'a pas de racine rationnelle.
❧ Considérons maintenant P_n comme une application polynomiale de $\mathbb{R}$ dans $\mathbb{R}$. Cette application est de classe $\mathscr{C}^2$ et

$$\forall\, x \in \mathbb{R}, \qquad P_n'(x) = nx^{n-1} - 1, \quad P_n''(x) = n(n-1)x^{n-2}.$$

Posons $r_n = (1/n)^{1/(n-1)} \in]0,1[$.
Si n est impair, alors la fonction P_n est croissante sur les intervalles

$$]-\infty, -r_n] \qquad \text{et} \qquad [r_n, +\infty[$$

et décroissante sur le segment $[-r_n, r_n]$. De plus,

$$P_n(-r_n) = -\left(\frac{1}{n}\right)^{n/(n-1)} + \left(\frac{1}{n}\right)^{1/(n-1)} - 1 < 0,$$

donc P_n est strictement négative sur $]-\infty, r_n]$. Sur l'intervalle $]r_n, +\infty[$, la fonction P_n est continue, strictement croissante et change de signe. Donc P_n admet une, et une seule, racine réelle.

✍ *Comme n est impair, $P_n(1) = -1 < 0$ et $P_n(2) = 2^n - 2 - 1 > 0$ (puisque $n \geqslant 2$), donc la racine réelle est comprise entre 1 et 2.*

Si n est pair, alors la fonction P_n est convexe sur $\mathbb{R}$ et atteint son minimum en r_n. Ce minimum est égal à

$$P_n(r_n) = \left(\frac{1}{n}\right)^{n/(n-1)} - \left(\frac{1}{n}\right)^{1/(n-1)} + 1 > 0$$

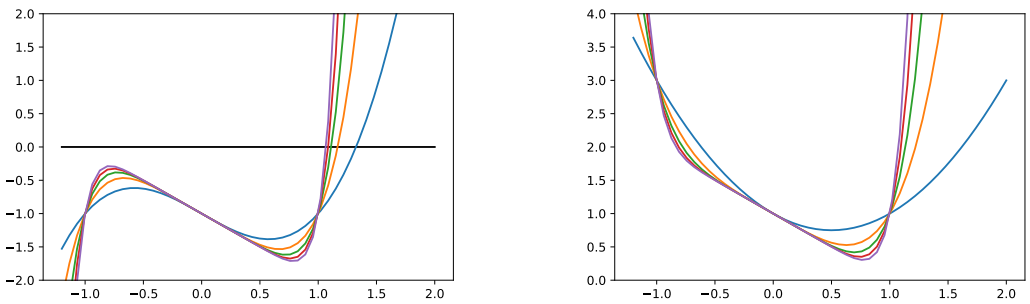
(le terme négatif est compris entre -1 et 0), donc P_n n'a pas de racine réelle.

✍ *On peut facilement vérifier les calculs précédents en définissant une fonctionnelle* `P` *(c'est-à-dire une fonction de* n *qui renvoie une fonction de* x*) et en traçant quelques graphes.*

```
def P(n):
    def Pn(x):
        return x**n-x+(-1)**n
    return Pn

U = np.linspace(-1.2, 2)

plt.figure()
plt.plot(U, np.zeros_like(U), 'k') # axe des abscisses
for k in range(1, 6):
    P_impair = P(2*k+1)
    plt.plot(U, P_impair(U))
plt.ylim(-2, 2)
plt.figure()
for k in range(1, 6):
    P_pair = P(2*k)
    plt.plot(U, P_pair(U))
plt.ylim(0, 4)
```



Graphes de quelques fonctions P_n avec n impair à gauche et n pair à droite

❧ Sur le corps $\mathbb{C}$, le polynôme P_n est scindé (son degré est supérieur à 2, donc il n'est pas constant). Par ailleurs, si $P_n'(z) = 0$, alors $z^{n-1} = 1/n$ et par conséquent

$$P_n(z) = z^n - z + (-1)^n = z\Big(\frac{1}{n} - 1\Big) + (-1)^n$$

et comme

$$0 \leqslant \Big|z\Big(\frac{1}{n} - 1\Big)\Big| = \Big(1 - \frac{1}{n}\Big)|z| = \Big(1 - \frac{1}{n}\Big)r_n < 1,$$

il est clair que $P_n(z) \neq 0$. D'après la deuxième question de cours, les racines complexes de P_n sont toutes simples, donc P_n possède exactement n racines complexes de multiplicité 1.
[**2.**] Comme P_n est un polynôme unitaire scindé de degré n,

$$P_n = \prod_{k=1}^{n}(X - a_k) = X^n - \Big(\sum_{k=1}^{n} a_k\Big)X^{n-1} + \cdots + (-1)^{n-1}\Big(\sum_{k=1}^{n}\prod_{\substack{1\leqslant \ell\leqslant n\\ \ell\neq k}} a_\ell\Big)X + (-1)^n\prod_{k=1}^{n} a_k.$$

On en déduit que la somme des racines est nulle et que

$$\sum_{k=1}^{n}\prod_{\substack{1\leqslant \ell\leqslant n\\ \ell\neq k}} a_\ell = \sum_{k=1}^{n}\prod_{\substack{1\leqslant \ell\leqslant n\\ \ell\neq k}} a_\ell = (-1)^n.$$

✍ *Les relations entre coefficients et racines d'un polynôme sont très utiles. À défaut de les connaître, il faut savoir les retrouver rapidement.*

❧ Le calcul qui suit est assez astucieux, mais cette astuce est plutôt classique. (Peut-être existe-t-il une méthode sans astuce pas trop compliquée ?)

❧ Considérons l'application polynomiale Q définie par

$$\forall\, x \in \mathbb{R}, \qquad Q(x) = \det(M - xI_n).$$

C'est, au signe près, le polynôme caractéristique de M, donc c'est un polynôme de degré n et son coefficient dominant est égal à $(-1)^n$.

Comme les scalaires a_k sont deux à deux distincts, la famille $(L_k)_{1\leqslant k\leqslant n}$ des polynômes interpolateurs de Lagrange est une base de $\mathbb{C}_{n-1}[X]$ et comme P_n est un polynôme unitaire de degré n, il existe n scalaires $(u_k)_{1\leqslant k\leqslant n}$ tels que

$$Q = (-1)^n P_n + \sum_{k=1}^{n} u_k L_k. \tag{$\star$}$$

On sait (cf cours sur l'interpolation de Lagrange) que $u_k = Q(a_k)$ pour $1 \leqslant k \leqslant n$.

Pour simplifier les notations, nous allons calculer $Q(a_1)$ et on donnera le résultat général qui s'en déduit.

$$Q(a_1) = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ & 1+a_2-a_1 & & \\ & & \ddots & \\ 1 & 1 & \cdots & 1+a_n-a_1 \end{vmatrix}$$

$$= \begin{vmatrix} 1 & 0 & \cdots & 0 \\ & a_2-a_1 & & \\ & & \ddots & \\ 1 & 0 & \cdots & a_n-a_1 \end{vmatrix} \qquad (C_j \leftarrow C_j - C_1 \text{ pour } 2 \leqslant j \leqslant n)$$

$$= \prod_{k=2}^{n} (a_k - a_1) \qquad \text{(matrice triangulaire)}$$

On se convainc aisément que

$$\forall\, 1 \leqslant k \leqslant n, \qquad Q(a_k) = \prod_{\substack{1\leqslant \ell\leqslant n \\ \ell\neq k}} (a_\ell - a_k)$$

et donc que, d'après $(\star)$ et la formule *bien connue* des polynômes interpolateurs de Lagrange,

$$Q = (-1)^n P_n + \sum_{k=1}^{n} \prod_{\substack{1\leqslant \ell\leqslant n \\ \ell\neq k}} (a_\ell - X).$$

En particulier,

$$\det M = Q(0) = (-1)^n P_n(0) + \sum_{k=1}^{n} \prod_{\substack{1\leqslant \ell\leqslant n \\ \ell\neq k}} a_\ell = 1 + (-1)^n.$$

Le déterminant de M est donc égal à 2 lorsque n est pair et à 0 lorsque n est impair.

✍ *Pour un polynôme P de la forme*

$$P = X^n + u_1 X^{n-1} + \cdots + u_{n-1} X + u_n$$

qui admet n racines $a_1, \ldots, a_n$ deux à deux distinctes dans $\mathbb{C}$, on trouverait de la même manière

$$\det M = \sum_{k=1}^{n} \prod_{\substack{1\leqslant \ell\leqslant n \\ \ell\neq k}} a_\ell + \prod_{k=1}^{n} a_k = (-1)^{n-1} u_{n-1} + (-1)^n u_n.$$

❧ *Si les racines complexes $a_1, \dots, a_n$ ne sont pas deux à deux distinctes, il suffit de constater que* $\det M$ *est en général une expression polynomiale des $a_1, \dots, a_n$ (avec la somme sur les permutations de $\mathfrak{S}_n$) et que deux polynômes qui sont égaux sur une partie dense de $\mathbb{C}^n$ sont en fait égaux sur $\mathbb{C}^n$. (Si on ne sait pas démontrer que les listes de n complexes deux à deux distinctes sont denses dans $\mathbb{C}^n$, on ne sait pas non plus démontrer que les matrices diagonalisable sont denses dans $\mathfrak{M}_n(\mathbb{C})$...)*

❧ *Il est facile de vérifier cette formule sur quelques exemples avec les modules habituels de Python.*

On part de la liste des racines complexes (pas nécessairement distinctes) pour définir le polynôme unitaire P.

```
def polynome(A):
    P = (X-A[0])
    for a in A[1:]:
        P *= (X-a)
    return P
```

La matrice M *est alors vite définie et son déterminant facilement calculé.*

```
def formule_verifiee(A):
    P = polynome(A)
    n = P.degree()
    M = np.ones((n, n))+np.diag(A)
    expr = (-1)**n*(P.coef[0]-P.coef[1])
    return (alg.det(M)-expr)
```

On peut vérifier sur des exemples variés que la différence entre le déterminant de M *et l'expression littérale*

$$(-1)^n(u_n - u_{n-1})$$

est très faible (de l'ordre de 10^{-17}) et seulement dûe aux invitables erreurs d'arrondi.

```
def coeffs_aleatoires():
    n = rd.randint(2, 10)
    A = rd.random(n+1)
    print(formule_verifiee(A))

for _ in range(20):
    coeffs_aleatoires()
```

[1.] *Soient* E, *un espace euclidien ;* f, *un endomorphisme de* E *et* $\mathscr{B} = (x_k)_{1\leqslant k\leqslant n}$, *une base orthonormée de* E. *Démontrer que*

$$\operatorname{tr} f = \sum_{k=1}^{n} \langle x_k \,|\, f(x_k)\rangle .$$

[2.] *Soient* M *et* N, *deux matrices symétriques positives.*
[2.a.] *Démontrer qu'il existe une matrice* $R \in \mathcal{S}_n^+(\mathbb{R})$ *telle que* $R^2 = M$. *En déduire que*

$$0 \leqslant \operatorname{tr}(MN).$$

[2.b.] *Démontrer que*

$$\operatorname{tr}(MN) \leqslant \operatorname{tr}(M).\operatorname{tr}(N).$$

[1.] Soit $A \in \mathfrak{M}_n(\mathbb{R})$, la matrice de f relative à la base orthonormée $\mathscr{B}$. Par définition,

$$\forall\, 1 \leqslant j \leqslant n, \qquad f(x_j) = \sum_{i=1}^{n} a_{i,j} \cdot x_i$$

et comme la base $\mathscr{B}$ est orthonormée,

$$\forall\, 1 \leqslant j \leqslant n, \qquad f(x_j) = \sum_{i=1}^{n} \big\langle x_i \,\big|\, f(x_j)\big\rangle \cdot x_i.$$

Par unicité de la décomposition d'un vecteur dans une base (orthonormée ou non !),

$$\forall\, 1 \leqslant i,j \leqslant n, \qquad a_{i,j} = \big\langle x_i \,\big|\, f(x_j)\big\rangle$$

et en particulier

$$\operatorname{tr} f = \sum_{i=1}^{n} a_{i,i} = \sum_{k=1}^{n} \langle x_k \,|\, f(x_k)\rangle .$$

[2.a.] Comme $M \in \mathcal{S}_n^+(\mathbb{R})$, il existe une matrice orthogonale P et une matrice diagonale $\Delta = \operatorname{Diag}(\alpha_1,\dots,\alpha_n)$ telles que

$$P^\top.M.P = P^{-1}.M.P = \Delta \quad \text{et} \quad \forall\, 1 \leqslant k \leqslant n, \quad \alpha_k \geqslant 0.$$

En posant $D = \operatorname{Diag}(\sqrt{\alpha_1},\dots,\sqrt{\alpha_n})$ et

$$R = P.D.P^\top = P.D.P^{-1},$$

on obtient une matrice $R \in \mathcal{S}_n^+(\mathbb{R})$ telle que $R^2 = M$.

❧ D'après la propriété fondamentale de la trace,

$$\operatorname{tr}(MN) = \operatorname{tr}(R.R.N) = \operatorname{tr}(R.N.R).$$

Or la matrice RNR est symétrique réelle et

$$\forall\, x \in \mathbb{R}^n, \qquad x^\top.(RNR).x = (Rx)^\top.N.(Rx) \geqslant 0$$

puisque $N \in \mathcal{S}_n^+(\mathbb{R})$. Donc $RNR \in \mathcal{S}_n^+(\mathbb{R})$: cette matrice est diagonalisable (Théorème spectral à nouveau) et ses valeurs propres sont positives, donc sa trace est positive.

On a ainsi démontré que $\operatorname{tr}(MN) \geqslant 0$.

[2.b.] Appliquons une fois encore le Théorème spectral à la matrice M et considérons une base orthonormée $(e_i)_{1\leqslant i\leqslant n}$ de vecteurs propres de M (associés aux valeurs propres $(\alpha_i)_{1\leqslant i\leqslant n}$).

D'après la première question et par symétrie de M,

$$\operatorname{tr}(MN) = \sum_{i=1}^{n} e_i^\top.(MN)e_i = \sum_{i=1}^{n} (Me_i)^\top.(Ne_i) = \sum_{i=1}^{n} \alpha_i \cdot e_i^\top.(Ne_i)$$

puisque $(Me_i) = \alpha_i \cdot e_i$. Comme $N \in \mathcal{S}_n^+(\mathbb{R})$,

$$\forall\, 1 \leqslant i \leqslant n, \qquad 0 \leqslant e_i^\top.(Ne_i) \leqslant \sum_{k=1}^{n} e_k^\top.(Ne_k) = \operatorname{tr}(N)$$

et comme les α_i sont positifs (ce sont les valeurs propres de $M \in \mathcal{S}_n^+(\mathbb{R})$),

$$\operatorname{tr}(MN) = \sum_{i=1}^{n} \alpha_i \cdot e_i^\top.(Ne_i) \leqslant \sum_{i=1}^{n} \alpha_i \operatorname{tr}(N) = \operatorname{tr}(M).\operatorname{tr}(N).$$

Soit $(G,*)$, un groupe fini d'élément neutre e. On suppose que

$$\forall\, x \in G, \qquad x^2 = e.$$

[**1.**] *Le groupe $(G,*)$ est abélien.*
[**2.**] *Soient H, un sous-groupe strict de G et $a \in G \setminus H$. On pose*

$$aH = \{a * x,\ x \in H\}.$$

[**2. a.**] *Les ensembles H et aH ont même cardinal.*
[**2. b.**] *Les ensembles H et aH sont disjoints.*
[**2. c.**] *L'ensemble $H \cup aH$ est un sous-groupe de G.*
[**3.**] *Le cardinal de G est une puissance de 2.*
[**4.**] *Calculer le produit des éléments de G.*

[**1.**] Soient g et h, deux éléments de G. Dans tout groupe, on sait que

$$(g*h)^{-1} = h^{-1} * g^{-1}.$$

Or, par hypothèse, $x^{-1} = x$ pour tout $x \in G$. En appliquant cette propriété à g, à h ainsi qu'à $(g*h)$, on obtient

$$g*h = (g*h)^{-1} = h*g.$$

Le groupe $(G,*)$ est donc commutatif.
[**2. a.**] Comme a admet un symétrique dans G, l'application $\varphi_a = [x \mapsto a*x]$ est une bijection de G dans G et cette bijection est même une involution :

$$\forall\, x \in G, \qquad \varphi_a\big(\varphi_a(x)\big) = a*(a*x) = a^2 * x = x.$$

✍ *Une **involution** est une bijection $f : G \to G$ qui est sa propre réciproque :*

$$\forall\, x \in G, \quad f^{-1}(x) = f(x) \quad \textit{c'est-à-dire} \quad \forall\, x \in G, \quad f\big(f(x)\big) = x.$$

Par exemple, toute symétrie centrale ou axiale est une involution.

L'application φ_a est donc injective.
❧ Par définition de aH, l'application φ_a induit une application surjective de H sur aH et comme φ_a est injective, l'application induite est une bijection de H sur aH.
❧ En particulier, les ensembles H et aH ont même cardinal.
[**2. b.**] Si $x \in H \cap aH$, alors il existe deux éléments h_1 et h_2 de H tels que

$$x = h_1 = a * h_2.$$

On en déduit en multipliant à droite par h_2^{-1} que

$$H \ni h_1 * h_2^{-1} = a \notin H$$

puisque H est un sous-groupe de $(G,*)$. C'est absurde, donc l'intersection $H \cap aH$ est vide.

✍ *En particulier, l'ensemble aH ne contient pas l'élément neutre e (qui appartient au sous-groupe H), donc aH n'est pas un sous-groupe de $(G,*)$.*

[**2. c.**] Il est clair que l'union $H \cup aH$ est contenue dans G.
❧ Comme H est un sous-groupe de $(G,*)$, on sait que

$$e \in H \subset H \cup aH.$$

❧ Soient x et y dans $H \cup aH$. Il faut démontrer que $x * y^{-1} \in H \cup aH$ et quatre cas se présentent. Il existe deux éléments h_1 et h_2 de H tels que :
— $x = h_1$ et $y = h_2$, donc $x * y^{-1} = h_1 * h_2^{-1} \in H$ puisque H est un sous-groupe ;
— $x = a * h_1$ et $y = h_2$, donc $x * y^{-1} = a * (h_1 * h_2^{-1}) \in aH$ puisque H est un sous-groupe ;

— $x = h_1$ et $y = ah_2$, donc $x * y^{-1} = h_1 * (h_2^{-1} * a^{-1}) = a * (h_1 * h_2)$ puisque $(G, *)$ est un groupe commutatif où tout élément est son propre symétrique et comme H est un sous-groupe, le produit $h_1 * h_2$ appartient à H et $x * y^{-1} \in aH$;
— $x = a * h_1$ et $y = a * h_2$, donc

$$x * y^{-1} = a * h_1 * h_2^{-1} * a^{-1} = a^2 * h_1 * h_2 = h_1 * h_2 \in H$$

pour les mêmes raisons.
Dans tous les cas, on a démontré que $x * y^{-1} \in H \cup aH$.
On a ainsi démontré que $H \cup aH$ était un sous-groupe de $(G, *)$.

[**3.**] On procède par récurrence.
❧ L'ensemble $H_0 = \{e\}$ est un sous-groupe de $(G, *)$ de cardinal $1 = 2^0$.
❧ HR : On suppose connu un sous-groupe H_n de $(G, *)$ de cardinal 2^n.
❧ Deux cas se présentent.
— Si $H_n = G$, alors le cardinal de G est une puissance de 2.
— Sinon, H_n est un sous-groupe strict de G et il existe donc $a_{n+1} \in G \setminus H_n$. D'après la question précédente, l'ensemble

$$H_{n+1} = H_n \cup a_{n+1} H_n$$

est un sous-groupe de $(G, *)$ et

$$\#(H_{n+1}) = \#(H_n) + \#(a_{n+1} H_n) = 2\#(H_n) = 2^{n+1}.$$

❧ Comme G est un ensemble fini, que $\#(H_n) = 2^n$ pour tout entier n tel que H_n soit défini et que la suite $(2^n)_{n\in\mathbb{N}}$ tend vers $+\infty$, il existe un rang N tel que H_N soit défini mais que H_{N+1} ne soit pas défini.
On en déduit alors que $G = H_N$ et donc que $\#(G) = 2^N$.

✍ *Exemples avec $\#(G) = 2$: $\{\pm 1\}$ en tant que sous-groupe de $(\mathbb{R}^*, \times)$ ou $\{\pm I_2\}$ en tant que sous-groupe du groupe $(SO_2(\mathbb{R}), \times)$ des rotations planes.*
Exemples avec $\#(G) = 4$:

$$\left\{ I_3, \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}$$

en tant que sous-groupe du groupe $(SO_3(\mathbb{R}), \times)$ des rotations de $\mathbb{R}^3$ ou le sous-groupe

$$V_4 = \{I, (\ 1\ \ 2\ ), (\ 3\ \ 4\ ), (\ 1\ \ 2\ )(\ 3\ \ 4\ )\}$$

en tant que sous-groupe du groupe symétrique $(\mathfrak{S}_4, \circ)$.

[**4.**] Comme l'opération $*$ est associative et commutative, on peut définir le produit des éléments de G sans qu'il soit nécessaire de préciser la position des différents facteurs (commutativité), ni la position des parenthèses qui détermine l'ordre chronologique des opérations (associativité).
❧ Puisque $H_{n+1} = H_n \cup a_n H_n$ et que H_n et $a_n H_n$ sont disjoints,

$$\prod_{x\in H_{n+1}} x = \left(\prod_{y\in H_n} y \right) * \left(\prod_{z\in a_n H_n} z \right) = \left(\prod_{y\in H_n} y \right) * \left(\prod_{y\in H_n} (a_n * y) \right).$$

Comme le groupe $(G, *)$ est abélien et que $y^2 = e$ pour tout $y \in G$,

$$\prod_{x\in H_{n+1}} x = a_n^{\#(H_n)} * \left(\prod_{y\in H_n} y^2 \right) = a_n^{\#(H_n)} = a_n^{2^n}.$$

❧ Si $G = H_0 = \{e\}$, alors le produit des éléments de G est égal à e !
Si $G = H_1$, alors $G = \{e, a_1\}$ avec $a_1 \neq e$ et le produit des éléments de G est égal à a_1.
Si $G = H_{n+1}$ avec $n \geqslant 1$, alors 2^n est un entier *pair*, donc $a_n^{2^n} = e$ et le produit des éléments de G est égal à e.