Méthodologie : énoncés

Preuves par l'absurde

1) Soit $f:\ [a,b]\to\mathbb{R}$ une fonction continue. Montrer que f est uniformément continue, i.e. que :

$$\forall\varepsilon>0,\ \exists\eta>0,\ \forall x,y\in[a,b],\ |x-y|\leq\eta\Longrightarrow|f(x)-f(y)|\leq\varepsilon.$$

2) Soient X un ensemble et $f:\ X\longrightarrow\mathcal{P}(X)$. Montrer que $A=\{x\in X,\ x\notin f(x)\}$ n'appartient pas à $f(X)$.

3) a) Montrer en utilisant une preuve par l'absurde que $\sqrt{2}$ n'est pas rationnel.

b) Montrer par contraposée que si $n\in\mathbb{N}$ n'est pas un carré parfait, $\sqrt{n}$ n'est pas rationnel (on pourra par exemple utiliser la décomposition des entiers en facteurs premiers).

4) Montrer par l'absurde qu'il existe une infinité de nombres premiers.

5) Soit $(E,\leq)$ un ensemble ordonnée. Montrer que les propriétés suivantes sont équivalentes :

(i) $\leq$ est un ordre total et toute suite décroissante d'éléments de E est stationnaire.

(ii) toute partie non vide de E a un plus petit élément.

Si ces propriétés sont vérifiées, on dit que $\leq$ est un *bon ordre*, ou que E est *bien ordonné* par $\leq$.

Montrer que $\mathbb{N}^{\mathbb{N}}$ n'est pas bien ordonné par l'ordre lexicographique.

6) Une clôture circulaire est constituée de 17 poteaux dont 5 sont pourris. Montrer qu'il existe un ensemble de 7 poteaux consécutifs dont 3 sont pourris.

Preuves par récurrence

7) Montrer par récurrence les propriétés :

$$\forall\, n\in\mathbb{N},\ \sum_{k=0}^{n}k^3=\frac{n^2(n+1)^2}{4}$$

$$\forall\, n\in\mathbb{N},\ \sum_{k=0}^{n}k^4=\frac{6n^5+15n^4+10n^3-n}{30}$$

8) Montrer que pour tout entier $n\geq 2$, $H_n=\displaystyle\sum_{k=1}^{n}\frac{1}{k}$ s'écrit $\dfrac{a_n}{b_n}$ avec a_n entier impair et b_n entier pair.

9) On considère l'application Δ de $\mathbb{R}^{\mathbb{N}}$ dans lui-même définie par :

$$\forall u\in\mathbb{R}^{\mathbb{N}},\ \forall n\in\mathbb{N},\ \left(\Delta(u)\right)_n=u_{n+1}-u_n.$$

Soit $f:\ [0,+\infty[\longrightarrow\mathbb{R}$ de classe C^∞ et u la suite définie par $\forall n\in\mathbb{N},\ u_n=f(n)$. Montrer la propriété :

$$\forall p\in\mathbb{N},\ \forall n\in\mathbb{N},\ \exists\, x\in[n,n+p],\ \left(\Delta^p(u)\right)_n=f^{(p)}(x).$$

10) Soit $f : \mathbb{R} \to \mathbb{R}$ de classe C^∞. On suppose qu'il existe un entier $k \geq 1$, k réels $a_1 < a_2 < \cdots < a_k$ et k entiers naturels non nuls $n_1, n_2, \ldots, n_k$ tels que :

$$\forall i \in \{1, \ldots, k\},\ \forall j \in \{0, \ldots, n_i - 1\},\ f^{(j)}(a_i) = 0.$$

Montrer qu'il existe $c \in \mathbb{R}$ tel que $f^{(N-1)}(c) = 0$, où $N = n_1 + \cdots + n_k$. Montrer que cette valeur N est maximale pour cette propriété (i.e. qu'il existe une fonction f vérifiant les hypothèse précédentes telle que $f^{(N)}$ ne s'annule pas sur $\mathbb{R}$.

11) Soit $G = (S, A)$ un graphe non orienté connexe. Montrer que $\mathrm{Card}(A) \geq \mathrm{Card}(S) - 1$. On donnera deux démonstrations : l'une par récurrence sur le nombre de sommets, l'autre par récurrence sur le nombre d'arêtes.

12) Démontrer que si $k \in \mathbb{N}^*$, si E est un K-espace vectoriel, si $\alpha, \beta_1, \ldots, \beta_k$ sont des formes linéaires sur E telles que $\bigcap_{i=1}^{k} \mathrm{Ker}\, \beta_i \subset \mathrm{Ker}\, \alpha$, alors $\alpha \in \mathrm{Vect}(\beta_1, \ldots, \beta_k)$.

13) Pour $n \in \mathbb{N}^*$ et $a_1, \ldots, a_n \in \mathbb{R}^{+*}$, on note :

$$D(a_1, \ldots, a_n) = \det \begin{pmatrix} a_1 & -1 & 0 & \ldots & 0 \\ 1 & a_2 & -1 & \ddots & \vdots \\ 0 & 1 & a_3 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & -1 \\ 0 & \ldots & 0 & 1 & a_n \end{pmatrix}$$

On définit par récurrence :

$$[a_1, \ldots, a_n] = \begin{cases} a_1 & \text{si } n = 1 \\ a_1 + \dfrac{1}{[a_2, \ldots, a_n]} & \text{si } n \geq 2 \end{cases}$$

Montrer que $[a_1, \ldots, a_n] = \dfrac{D(a_1, \ldots, a_n)}{D(a_2, \ldots, a_n)}$ pour tout $n \geq 2$.

14) Soient $n \in \mathbb{N}^*$, $b_1, \ldots, b_n$ des réels deux à deux distincts et $a_1, \ldots, a_n$ des réels non tous nuls. Montrer que la fonction $f : x \longmapsto \sum_{k=1}^{n} a_k e^{b_k x}$ s'annule au plus $n - 1$ fois.

Preuves d'existence

15) Soient $a, b \in \mathbb{R}$ avec $b \neq 0$. Montrer qu'il existe un et un seul réel θ tel que :

- $\theta \in]-\pi/4, 0[\cup]0, \pi/4]$;
- $a \sin\theta \cos\theta + b(\cos^2\theta - \sin^2\theta) = 0$.

16) On note Σ_1 le lieu des points $M(t, \theta) = \begin{pmatrix} t + \cos\theta \\ -t + \sin\theta \\ \sin(2\theta) \end{pmatrix}$ pour t, θ décrivant $\mathbb{R}$.

a) Montrer que Σ_1 est contenu dans la surface Σ_2 d'équation cartésienne $z = (x + y)^2 - 1$.

b) Étudier l'inclusion réciproque.

17) Soit I un intervalle et E l'espace vectoriel des applications définies sur I et à valeurs réelles. On note F le sous-espace vectoriel de E engendré par les applications croissantes.

a) Montrer que $f : I \to \mathbb{R}$ est élément de E si et seulement s'il existe g et h dans E avec $f = g + h$, g croissante et h décroissante.

b) Montrer que si $f \in F$ et si $\alpha \in I$, il existe g et h dans E vérifiant, en plus des conditions précédentes, la propriété $g(\alpha) = 0$.

18) Soit $f : [0,1] \to \mathbb{R}$ une application continue. Montrer que f possède une unique primitive F telle que $\displaystyle\int_0^1 F(x)\,\mathrm{d}x = 0$.

19) Montrer que les relations : $c_1 = 0$, $\lambda_1 = 2$ et $\forall\, n \geq 1,\ c_{n+1} = \sqrt{\dfrac{1+c_n}{2}}$ et $\lambda_{n+1} = \dfrac{\lambda_n}{c_{n+1}}$ permettent bien de définir les suites $(c_n)_{n\geq 1}$ et $(\lambda_n)_{n\geq 1}$.

20) Soit $(K, +, \cdot)$ un corps.

a) Montrer qu'il existe un unique morphisme d'anneau $\varphi : \mathbb{Z} \longrightarrow K$. Le noyau de φ est un idéal de $\mathbb{Z}$, il est donc de la forme $c\mathbb{Z}$ avec $c \in \mathbb{N}$.

b) On suppose que φ est injectif, i.e. que $c = 0$. Montrer qu'il existe un unique morphisme d'anneau $\widetilde{\varphi} : \mathbb{Q} \longrightarrow K$ qui prolonge φ et que ce morphisme est injectif.

c) On suppose que c est non nul. Montrer qu'il existe un unique morphisme d'anneau $\widetilde{\varphi} : \mathbb{Z}/c\mathbb{Z} \longrightarrow K$. Montrer que $\widetilde{\varphi}$ est injectif. En déduire que c est un nombre premier.

Exercices divers

21) Dénombrer les surjections de $\{1, 2, \ldots, n+1\}$ dans $\{1, 2, \ldots, n\}$.

22) Si E et F sont deux ensembles, on note $E \sim F$ pour signifier que E et F sont *équipotents*, i.e. qu'il existe une bijection de E sur F. On rappelle également que l'ensemble des applications de E dans F est noté F^E.

Soient A, B, C et D des ensembles. Montrer les propriétés suivantes :

- $A \sim A$
- $A \sim B \Longrightarrow B \sim A$
- $(A \sim B \text{ et } B \sim C) \Longrightarrow A \sim C$
- $A \sim B \Longrightarrow \mathcal{P}(A) \sim \mathcal{P}(B)$
- $C^{A\times B} \sim \left(C^A\right)^B$
- $(A \sim C \text{ et } B \sim D) \Longrightarrow \left(A \times B \sim C \times D \text{ et } A^B \sim C^D\right)$

23) Quels sont les éléments minimaux de $\mathbb{N} \setminus \{0,1\}$ muni de l'ordre : $n \leq m$ ssi n divise m ?

24) Théorème de Cantor-Bernstein

Soit $f : E \to F$ et $g : F \to E$ deux injections. On note g^{-1} la bijection de $g(F)$ sur F qui, à $x \in g(F)$, associe l'unique élément y de F tel que $g(y) = x$. On pose :

$$A_0 = E \setminus g(F) \qquad \text{et} \qquad \forall n \geq 1, \begin{cases} B_n = f(A_{n-1}) \\ A_n = g(B_n) \end{cases}$$

On définit alors $\phi : E \to F$ par $\forall x \in E, \phi(x) = \begin{cases} f(x) & \text{si } x \in \bigcup_{n\geq 0} A_n, \\ g^{-1}(x) & \text{sinon.} \end{cases}$

Montrer que ϕ est une bijection.

25) Soit E un ensemble et $f : E \to \mathcal{P}(E)$. Soit A la partie de E définie par la relation

$$\forall x \in E, \quad x \in A \iff x \notin f(x).$$

Montrer que $A \notin f(E)$ et en déduire que le cardinal de $\mathcal{P}(E)$ est toujours strictement plus grand que celui de E. Pourquoi ne peut-on pas parler de l'ensemble de tous les ensembles ?

26) Montrer que les ensembles $\mathbb{Z}$, $\mathbb{N}^2$ et $\mathbb{Q}$ sont dénombrables, i.e. qu'ils peuvent être mis en bijection avec $\mathbb{N}$. Montrer que $\mathbb{R}$, $\mathbb{R}^2$ et $\mathbb{R}^{\mathbb{N}}$ sont équipotents à $\{0,1\}^{\mathbb{N}}$, puis à $\mathcal{P}(\mathbb{N})$. En déduire que $\mathbb{R}$ n'est pas dénombrable.

27) Montrer que $\mathbb{Q}$ et $\mathbb{Q}[X]$ sont dénombrables, et en déduire que l'ensemble des nombres complexes algébriques [1] est dénombrable. Que peut-on dire de l'ensemble des nombres transcendants ?

28) Soit $D = \{x_n,\ n \in \mathbb{N}\}$ une partie dénombrable de $\mathbb{R}$. En utilisant les écritures décimales des x_n, construire un réel x n'appartenant pas à D. En déduire que $\mathbb{R}$ n'est pas dénombrable.

29) (Centrale 2012) Déterminer le max et le min, lorsque σ parcourt l'ensemble des permutations de $\{1,\dots,n\}$, de $\displaystyle\sum_{k=1}^{n} k\,\sigma(k)$.

30) Soient $(E_1, \leq_1)$ et $(E_2, \leq_2)$ deux ensembles bien ordonnés (un ensemble bien ordonné est un ensemble ordonné dans lequel toute partie non vide possède un plus petit élément).

a) On suppose que E_1 et E_2 sont disjoints (quitte à faire une "copie" de E_2) et on note $E = E_1 + E_2$ l'ensemble $E_1 \sqcup E_2$ muni de l'ordre :

$$a \leq b \iff \big((a \in E_1 \text{ et } b \in E_2) \text{ ou } (a, b \in E_1 \text{ et } a \leq_1 b) \text{ ou } (a, b \in E_2 \text{ et } a \leq_2 b)\big).$$

Montrer que $E_1 + E_2$ est bien ordonné, et que $E_1 + E_2$ et $E_2 + E_1$ ne sont pas isomorphes [2] en général.

b) Montrer que le produit cartésien $E_1 \times E_2$ est bien ordonné par l'ordre lexicographique et que $E_1 \times E_2$ et $E_2 \times E_1$ ne sont pas isomorphes en général.

Exercices X-ENS

31) (X) Soit X un ensemble, $n \in \mathbb{N}^*$ et $X_1, \dots, X_n$ des parties de X. Pour tout $k \in [\![1, n]\!]$, on note $\mathcal{P}_k$ l'ensemble des parties de $[\![1, n]\!]$ de cardinal k et on pose $Y_k = \displaystyle\bigcup_{I \in \mathcal{P}_k} \left(\bigcap_{i \in I} X_i \right)$ et $Z_k = \displaystyle\bigcap_{I \in \mathcal{P}_k} \left(\bigcup_{i \in I} X_i \right)$. À quelle condition sur k a-t-on $Y_k \subset Z_k$ (resp. $Z_k \subset Y_k$) ?

32) (X) Soit E un ensemble fini non vide muni d'une loi de composition interne associative $*$. Montrer qu'il existe un élément $e \in E$ tel que $e * e = e$.

33) (X) Soit E un ensemble. Montrer que E est infini si et seulement si pour toute fonction $f : E \longrightarrow E$, il existe une partie A de E telle que $A \neq \emptyset$, $A \neq E$ et $f(A) \subset A$.

34) Soit σ une permutation de $\mathbb{N}$. On note $A = \{n \in \mathbb{N},\ \sigma(n) \geq n\}$ et $B = \{n \in \mathbb{N},\ \sigma(n) < n\}$.

1. Un nombre complexe est dit *algébrique* s'il est racine d'un polynôme non nul à coefficients entiers. Les nombres complexes non algébriques sont dits *transcendants*
2. Deux ensemble ordonnés sont dits isomorphes s'il existe une bijection f de l'un sur l'autre telle que f et f^{-1} soient croissantes. Attention : f peut être bijective et croissante sans que f^{-1} ne soit croissante !

a) Est-il possible que B soit fini ?

b) Est-il possible que A et B soient infinis ?

c) Est-il possible que A soit fini ?

35) (L 2017)Soit $n \in \mathbb{N}^*$. Déterminer k maximal tel qu'il existe $E_1, \ldots, E_k$ parties de $\{1, 2, \ldots, n\}$ telles que :

$$\begin{cases} \forall i \in \{1, 2, \ldots, k\},\ |E_i| \text{ est impair} \\ \\ \forall i, j \in \{1, 2, \ldots, k\},\ |E_i \cap E_j| \text{ est pair si } i \neq j \end{cases}$$

36) (ENS) Montrer que $\mathfrak{S}_{\mathbb{Q}}$ n'est pas dénombrable.

Indication : on pourra construire une application injective de $\mathbb{R}$ dans $\mathfrak{S}_{\mathbb{Q}}$.

Méthodologie : corrigés

Preuves par l'absurde

1) Supposons que la propriété soit fausse. Il existe donc $\varepsilon_0 > 0$ tel que :

$$\forall \eta > 0,\ \exists x, y \in [a,b],\ |x-y| \leq \eta \text{ et } |f(x)-f(y)| > \varepsilon_0.$$

Pour tout entier $n \geq 1$, on peut choisir $\eta = 1/n$ et il existe ainsi $x_n, y_n \in [a,b]$ tels que $|x_n - y_n| > \eta$ et $|f(x_n) - f(y_n)| > \varepsilon_0$.

La suite réelle $(x_n)_{n\geq 1}$ est bornée : le théorème de Bolzano-Weierstrass prouve qu'il existe une fonction $\varphi : \mathbb{N} \to \mathbb{N}^*$ strictement croisante et $x \in \mathbb{R}$ telle que $x_{\varphi(n)}$ converge vers x quand n tend vers l'infini. Comme $y_{\varphi(n)} - x_{\varphi(n)}$ tend vers 0 quand n tend vers l'infini, la suite $(y_{\varphi(n)})_{n\in\mathbb{N}}$ tend également vers x. Nefin, $x \in [a,b]$ et f est continue, donc (caractérisation séquentielle de la continuité) $f(x_{\varphi(n)})$ et $f(y_{\varphi(n)})$ tendent vers $f(x)$ quand n tend vers l'infini. En faisant tendre n vers l'infini dans l'inégalité $|f(x_{\varphi(n)}) - f(y_{\varphi(n)})| > \varepsilon_0$, nous obtenons l'absurdité $0 \geq \varepsilon_0$.

2) Supposons que A appartienne à $f(X)$. Il existe alors $x_0 \in X$ tel que $A = f(x_0)$. Nous devons mettre en évidence une absurdité dans cette situation très pauvre, où nous disposons d'un élément x_0 de X et d'une partie A de X : il est naturel de se poser la question de l'appartenance de x_0 à A. Nous avons :

$$x_0 \in A \iff x_0 \notin f(x_0) \iff x_0 \notin A$$

ce qui est absurde.

3) a) Supposons que $\sqrt{2}$ soit égal à $\dfrac{p}{q}$ avec $p, q \in \mathbb{N}^*$ tels que $p \wedge q = 1$. Nous avons alors $p^2 = 2q^2$, donc p est pair. On en déduit que p^2 est divisible par 4, c'est-à-dire que q^2 est pair ; ainsi, q est pair : c'est absurde car cela contredit l'hypothèse $p \wedge q = 1$.

Remarque : avant Euclide, la notion de nombre premiers entre eux n'était pas connue, et on peut imaginer la preuve un peu différente suivante. Si $p^2 = 2q^2$ avec $p, q \in \mathbb{N}^*$, alors p est pair, puis q est pair, puis p est multiple de 4, puis q est multiple de 4, et par itération, p est multiple de toutes les puissances de 2 : c'est absurde.

À l'époque des grecs anciens, les "nombres" se devaient d'être des rapports de longueurs entières, i.e. des nombres rationnels positifs ... mais parallèlement, les nombres étaient sensés représenter les longueurs et les aires des objets de la géométrie usuelle (constructible à la règle et au compas). Ainsi, il devait exister un nombre dont le carré était égal à 2 (longueur de la diagonale d'un carré de côté 1), ce qui semblait paradoxal puisqu'un tel "nombre" ne pouvait exister. Comme cela s'est reproduit de nombreuses fois dans l'histoire des mathématiques, les grecs anciens mettaient ainsi en évidence l'incohérence de leur modèle mathématiques (ici, la double vision des nombres).

b) Supposons que $n \in \mathbb{N}$ soit tel que $\sqrt{n} \in \mathbb{Q}$. Il existe alors deux entiers naturels a et b tels que $a^2 = nb^2$. Chaque nombre entier peut se décomposer d'une unique façon en produit de facteurs premiers : nous noterons, pour tout $k \in \mathbb{N}$ et pour tout $p \in \mathbf{P}$ nombre premier, $v_p(k)$ l'exposant de p dans la décomposition de k ($v_p(k)$ est la *valuation p-adique* de k). Ainsi :

$$\forall k \in \mathbb{N},\ k = \prod_{p\in\mathbf{P}} p^{v_p(k)}.$$

On montre facilement que $v_p(k_1 k_2) = v_p(k_1) v_p(k_2)$ pour tous $k_1, k_2 \in \mathbb{N}$ et $p \in \mathbf{P}$, et donc :

$$\forall p \in \mathbf{P},\ 2v_p(a) = v_p(n) + 2v_p(b).$$

On en déduit que $v_p(n)$ est un entier naturel pair pour tout $p \in \mathbf{P}$, et donc que n est un carré parfait.

Nous avons donc montré par contraposée que si n n'est pas un carré parfait, $\sqrt{n}$ est irrationnel.

4) Supposons qu'il n'existe qu'un nombre fini de nombres premiers, notés $p_1, \ldots, p_n$. Alors le nombre $N = 1 + p_1 p_2 \ldots p_n$ possède au moins un diviseur premier, ce qui est absurde puisqu'aucun des p_i ne divise N.

On peut transformer cette preuve par l'absurde en preuve par récurrence, on démontrant la propriété : pour tout $n \in \mathbb{N}^*$, il existe n nombres premiers distincts. L'initialisation est évidente ($p_1 = 2$ est premier) et si, pour $n \in \mathbb{N}^*$, on sait qu'il existe n nombres premiers distincts $p_1, \ldots, p_n$, alors $N = 1 + p_1 p_2 \ldots p_n$ possède un diviseur premier p_{n+1}, qui est distincts de p_1, p_2, ..., p_n : il existe ainsi $n+1$ nombres premiers distincts.

5) Supposons que (i) est vérifiée et supposons qu'il existe une partie A de E non vide et sans plus petit élément. Comme A est non vide, on peut fixer $a_0 \in A$. Comme a_0 n'est pas minimum de A, il existe un élément a_1 de A tel que $a_0 \not\leq a_1$. Comme l'ordre est total, on a $a_1 < a_0$. On construit ainsi par récurrence une suite $(a_n)_{n\in\mathbb{N}}$ strictement décroissante, ce qui contredit (i).

Supposons que (ii) est vérifié.

- Si a et b sont deux éléments de E, la partie $\{a, b\}$ possède un plus petit élément, donc soit $a \leq b$, soit $b \leq a$: l'ordre est total.
- Supposons qu'il existe une suite strictement décroissante $(a_n)_{n\in\mathbb{N}}$. La partie $A = \{a_n,\ n \in \mathbb{N}\}$ possède un plus petit élément m. Comme $m \in A$, il existe $n_0 \in \mathbb{N}$ tel que $m = a_{n_0}$, ce qui contredit la minimalité de m car $a_{n_0+1} < a_{n_0} = m$.

Remarque : la première preuve est en fait une preuve par contraposition (nous avons montré que si (ii) n'est pas vérifié et si l'ordre est total, alors il existe une suite strictement décroissante) mais la seconde est une vraie preuve par l'absurde, puisque nous avons eu besoin d'utiliser à la fois (ii) et l'existence d'une suite strctepent décroissante.

6) Notons $P_0, \dots, P_{16}$ les poteaux, numérotés dans un ordre circulaire. Pour $i \in \{0, \dots, 16\}$, notons N_i le nombre de poteaux pourris dans la suite des 7 poteaux consécutifs commençant à P_i. Comme chaque poteau pourri est compté 7 fois, nous avons :

$$\sum_{i=0}^{16} N_i = 5 \times 7 = 35.$$

On remarque que pour deux poteaux voisins P_i et P_{i+1}, $N_i - N_{i+1} \in \{-1, 0, 1\}$. Ainsi, s'il n'existe pas d'entier i tel que $N_i = 3$, on a soit $N_i \leq 2$ pour tout i, soit $N_i \geq 4$ pour tout i. On obtient donc :

$$\text{soit } 35 = \sum_{i=0}^{16} N_i \leq 17 \times 2 = 34, \text{ soit } 35 = \sum_{i=0}^{16} N_i \geq 17 \times 4 = 68$$

ce qui est absurde : il existe bien une suite de 7 poteaux consécutifs dont 3 sont pourris.

Preuves par récurrence

7) Pour $n \in \mathbb{N}$, notons A_n et B_n les deux membres de l'égalité. Nous avons $A_0 = 0 = B_0$ donc la propriété $\mathcal{P}_n$: $A_n = B_n$ est vérifiée au rang $n = 0$. Soit $n \in \mathbb{N}$ et supposons que $\mathcal{P}_n$ est vérifiée. Nous avons alors :

$$A_{n+1} = A_n + (n+1)^3 = B_n + (n+1)^3 = \frac{n^2(n+1)^2}{4} + (n+1)^3 = \frac{(n+1)^2}{4}\left(n^2 + 4(n+1)\right) = B_{n+1}$$

ce qui prouve l'hérédité de la propriété : $A_n = B_n$ est vraie pour tout $n \in \mathbb{N}$.

Le preuve est identique pour démontrer la seconde égalité, avec des calculs plus compliqués : pour l'hérédité, nous avons :

$$\begin{cases} A_{n+1} = \dfrac{6n^5 + 15n^4 + 10n^3 - n}{30} + n^4 + 5n^3 + 10n^2 + 5n + 1 = \dfrac{6n^5 + 45n^4 + 130n^3 + 180n^2 + 119n + 30}{30} \\ \\ B_{n+1} = \dfrac{6(n+1)^5 + 15(n+1)^4 + 10(n+1)^3 - (n+1)}{30} = \dfrac{6n^5 + 45n^4 + 130n^3 + 180n^2 + 119n + 30}{30} \end{cases}$$

et donc $A_{n+1} = B_{n+1}$ dès que $A_n = B_n$.

8) La preuve est un peu délicate. Il faut faire une récurrence forte couplée à une disjonction des cas (selon que n est pair ou impair), un des cas demandant en plus une petite astuce.

$H_2 = \dfrac{3}{2}$ avec 3 impair et 2 pair : la propriété demandée est vraie pour $n = 2$.

Soit $n \geq 2$ et supposons que la propriété demandée est vérifiée pour tout $k \in \{2, 3, \dots, n\}$.

- Si n est pair, on a :
$$H_{n+1} = H_n + \frac{1}{n+1} = \frac{a_n}{b_n} + \frac{1}{n+1} = \frac{a_n(n+1)+b_n}{(n+1)b_n}$$
avec a_n et b_n entiers naturels respectivement impair et pair. On a alors $a_n(n+1)+b_n$ est impair et $(n+1)b_n$ est pair.

- Sinon, il existe $q \geq 2$ tel que $n+1 = 2q$. On a alors, en séparant les termes pairs et impairs :
$$H_{n+1} = \sum_{k=1}^{2q} \frac{1}{k} = \frac{1}{2}\sum_{k=1}^{q} \frac{1}{k} + \sum_{k=1}^{q} \frac{1}{2k-1} = \frac{1}{2}\frac{a_q}{b_q} + \frac{N}{a}$$
avec a_q impair, b_q pair (hypothèse de récurrence appliquée à H_q, c qui est licite car $2 \leq q \leq n$), $N \in \mathbb{N}$ et $a = \prod_{k=1}^{q}(2k-1)$ impair. On a enfin :
$$H_{n+1} = \frac{a_q y + 2b_q N}{2b_q a}$$
avec $a_q y + 2b_q N$ impair (car a_q et y le sont et $2b_q N$ est pair) et $2b_q a$ pair.

Dans les deux cas, la propriété est vérifiée au rang $n+1$.

9) Nous allons faire une récurrence sur p, mais l'astuce consiste, pour passer à la propriété au rang $p+1$, d'appliquer la propriété au rang p à une autre fonction que f. Nous noterons donc, pour $f \in C^\infty(\mathbb{R}^+,\mathbb{R})$, u^f la suite $(f(n))_{n\in\mathbb{N}}$. Pour $p \in \mathbb{N}$, nous considérons la propriété :
$$\mathcal{P}_p : \ \forall f \in C^\infty(\mathbb{R}^+,\mathbb{R}),\ \forall n \in \mathbb{N},\ \exists x \in [n, n+p],\ \left(\Delta^p(u^f)\right)_n = f^{(p)}(x).$$

La propriété $\mathcal{P}_0$ est trivialement vérifiée : pour $f \in C^\infty(\mathbb{R}^+,\mathbb{R})$ et $n \in \mathbb{N}$, on choisit $x = n$ et on a bien $x \in [n, n+0]$ et $\left(\Delta^p(u^f)\right)_n = (u^f)_n = f(n) = f^{(0)}(x)$.

Soit $p \in \mathbb{N}$ et supposons que $\mathcal{P}_p$ est vérifiée. Soit $f \in C^\infty(\mathbb{R}^+,\mathbb{R})$ et $n \in \mathbb{N}$. On a alors $\Delta(u^f) = u^g$, en notant $g : x \longmapsto f(x+1) - f(x)$. Comme $g \in C^\infty(\mathbb{R}^+,\mathbb{R})$, on peut appliquer le propriété $\mathcal{P}_p$: il existe $x \in [n, n+p]$ tel que $(\Delta^p(u^g))_n = g^{(p)}(x)$, ce qui s'écrit aussi :
$$\left(\Delta^{p+1}(u^f)\right)_n = g^{(p)}(x) = f^{(p)}(x+1) - f^{(p)}(x).$$

On peut enfin appliquer le théorème des accroissement finis à $f^{(p)}$ sur $[x, x+1]$: il existe $y \in [x, x+1]$ tel que $f^{(p)}(x+1) - f^{(p)}(x) = (x+1-x)f^{(p+1)}(y) = f^{(p+1)}(y)$. On a donc montré l'existence d'un élément y dans $[n, n+p+1]$ tel que $\left(\Delta^{p+1}(u^f)\right)_n = f^{(p+1)}(y)$: $\mathcal{P}_{p+1}$ est vérifiée.

Remarque : il y a une démarche plus naturelle, mais qui ne fonctionne pas. On peut écrire :
$$\left(\Delta^{p+1}(u^f)\right)_n = \left(\Delta^p(u^f)\right)_{n+1} - \left(\Delta^p(u^f)\right)_n = f^{(p)}(x) - f^{(p)}(y)$$
avec $x, y \in [n, n+p]$, en appliquant deux fois $\mathcal{P}_p$ à f ... mais on ne peut pas conclure. Ainsi, le bon "découpage" de Δ^{p+1} est $\Delta^p \circ \Delta$ et pas $\Delta \circ \Delta^p$.

10) Pour $N \geq 1$, notons $\mathcal{H}_N$ la propriété :
$$\forall f \in \mathcal{C}^\infty(\mathbb{R},\mathbb{R}),\ \forall k \in \mathbb{N}^*,\ \forall a_1 < a_2 < \cdots < a_k \in \mathbb{R},\ \forall n_1, n_2, \ldots, n_k \in \mathbb{N} \text{ t.q. } n_1 + n_2 + \cdots + n_k = N,$$
$$\Big(\forall i \in \{1,\ldots,k\},\ \forall j \in \{0,\ldots n_i - 1\}, f^{(j)}(a_i) = 0\Big) \Longrightarrow \exists c \in \mathbb{R},\ f^{(N-1)}(c) = 0.$$

La propriété H_1 est trivialement vérifiée (si $f(a_1) = 0$, alors $f^{(0)}(c) = 0$ avec $c = a_1$).

Soit $N \geq 1$ et supposons H_N vraie. Soit f, $k \in \mathbb{N}^*$, $a_1 < a_2 < \cdots < a_k$ et $n_1, n_2, \ldots, n_k \in \mathbb{N}$ tels que
$$n_1 + n_2 + \cdots + n_k = N+1 \text{ et } \forall i \in \{1,\ldots,k\},\ \forall j \in \{0,\ldots n_i - 1\}, f^{(j)}(a_i) = 0.$$

Quitte à supprimer les a_i tels que $n_i = 0$, nous pouvons supposer que $n_i \geq 1$ pour tout i. Le théorème de Rolle peut alors être appliqué à f sur chaque intervalle $[a_i, a_{i+1}]$, pour $1 \leq i \leq k-1$. Nous obtenons ainsi des réels $b_1, \dots b_{k-1}$ tels que $a_1 < b_1 < a_2 < b_2 < \cdots < a_{k-1} < b_{k-1} < a_k$ et $f'(b_1) = \cdots = f'(b_{k-1}) = 0$. On peut alors appliquer H_{N-1} à l'application $g = f'$, en posant :

$$c_1 = a_1 < c_2 = b_1 < \cdots < c_{2k-3} = a_{k-1} < c_{2k-2} = b_{k-1} < c_{2k-1} = a_k$$

$$m_1 = n_1 - 1,\ m_2 = 1,\ \dots,\ m_{2k-3} = n_{k-1} - 1,\ m_{2k-2} = 1,\ m_{2k-1} = n_k - 1$$

On a en effet $m_1 + m_2 + \cdots + m_{2k-1} = n_1 + \cdots + n_k - k + k - 1 = N$ et

$$\forall i \in \{1, \dots, 2k-1\},\ \forall j \in \{0, \dots m_i - 1\}, g^{(j)}(c_i) = 0.$$

On en déduit qu'il existe $c \in \mathbb{R}$ tel que $g^{(N-1)}(c) = 0$, i.e. tel que $f^{(N)}(c) = 0$: ceci prouve que la propriété est héréditaire.

11) Récurrence sur le cardinal de S. Si G n'a qu'un sommet, on a $A = \emptyset$ et $\mathrm{Card}(A) = 0 = \mathrm{Card}(S) - 1$.

Soit S un graphe connexe à $n \geq 2$ sommets et supposons que tout graphe connexe possédant strictement moins de n sommets vérifie la relation. Soit $s \in S$ et notons $G' = (S', A')$ le graphe obtenu en supprimant de G le sommet s (et les arêtes incidentes à s). G' est alors réunion de graphes connexes : on peut partitionner $S = S_1 \sqcup \cdots \sqcup S_k$, $A = A_1 \sqcup \cdots \sqcup A_k$ où les S_i sont les composantes connexes de G' et $A_i = \{\{a, b\} \in A',\ a, b \in S_i\}$. On peut appliquer l'hypothèse de récurrence aux graphes (S_i, A_i) :

$$\forall i \in [\![1, k]\!],\ \mathrm{Card}(A_i) \geq \mathrm{Card}(S_i) - 1.$$

D'autre part, le graphe G étant connexe, il existe pour tout $i \in [\![1, k]\!]$, un sommet $s_i \in S_i$ tel que $(s, s_i) \in A$. Ainsi, il existe au moins k arêtes distinctes dans $A \setminus A'$, ce qui donne :

$$\mathrm{Card}(A) \geq k + \mathrm{Card}(A') = k + \sum_{i=1}^{k} \mathrm{Card}(A_i) \geq k + \sum_{i=1}^{k} (\mathrm{Card}(S_i) - 1) = \sum_{i=1}^{k} \mathrm{Card}(S_i) = \mathrm{Card}(S) - 1$$

et le résultat est démontré au rang $n + 1$.

Récurrence sur le cardinal de A. Si A est vide, G a au plus un sommet et on a bien $\mathrm{Card}(A) = 0 = \mathrm{Card}(S) - 1$.

Soit $n \geq 1$ et supposons le résultat démontré pour tout graphe connexe possédant strictement moins de n arêtes. Soit G un graphe connexe à n arêtes. Soit $a = \{s, t\}$ une arête de G et $G' = (S, A \setminus \{c\})$. Si G' est connexe, on peut lui appliquer l'hypothèse de récurrence :

$$\mathrm{Card}(A) \geq \mathrm{Card}(A') \geq \mathrm{Card}(S) - 1.$$

Sinon, G' possède deux composantes connexes : celle de s et celle de t. On peut alors appliquer l'hypothèse de récurrence aux deux graphes G_1 et G_2 définis en restreignant G' à ces deux composantes connexes : $G_1 = (S_1, A_1)$ et $G_2 = (S_2, A_2)$ sont connexes et on a :

$$S = S_1 \sqcup S_2,\ A = S_1 \sqcup S_2 \sqcup \{a\}$$

avec

$$\mathrm{Card}(A) = 1 + \mathrm{Card}(A_1) + \mathrm{Card}(A_2) \geq 1 + \mathrm{Card}(S_1) - 1 + \mathrm{Card}(S_2) - 1 = \mathrm{Card}(S) - 1.$$

12) Nous allons faire une récurrence sur k.

Initialisation : on suppose que α et β sont deux formes linéaires sur E telles que $\mathrm{Ker}\,(\beta) \subset \mathrm{Ker}\,(\alpha)$. Si $\alpha = 0$, on a bien $\alpha \in \mathrm{Vect}(\beta)$; sinon, $H = \mathrm{Ker}\,(\alpha)$ est un hyperplan et on peut fixer $x_0 \in E$ tel que $H \oplus \mathbb{K}x_0 = E$. On a alors $\beta(x_0) \neq 0$ (car x_0 n'est pas dans H et H contient $\mathrm{Ker}\,(\beta)$) et $\alpha = \dfrac{\alpha(x_0)}{\beta(x_0)}\beta$ (les deux formes linéaires coïncident sur H et en x_0).

Hérédité : soit $k \geq 1$ et supposons la propriété vraie au rang k. Soient E est un K-espace vectoriel et $\alpha, \beta_1, \dots, \beta_{k+1}$ des formes linéaires sur E telles que $\bigcap_{i=1}^{k+1} \mathrm{Ker}\beta_i \subset \mathrm{Ker}\alpha$. Considérons alors $F = \mathrm{Ker}\,(\beta_{k+1})$ et notons $\alpha', \beta_1', \dots, \beta_k'$ les restrictions de $\alpha, \beta_1, \dots, \beta_k$ à F. On a :

$$\bigcap_{i=1}^{k} \mathrm{Ker}\,(\beta_i') = \bigcap_{i=1}^{k} (\mathrm{Ker}\,(\beta_i) \cap \mathrm{Ker}\,(\beta_{k+1})) = \bigcap_{i=1}^{k+1} \mathrm{Ker}\,(\beta_i)$$

et $\mathrm{Ker}\,(\alpha') = \mathrm{Ker}\,(\alpha) \cap \mathrm{Ker}\,(\beta_{k+1})$, donc

$$\bigcap_{i=1}^{k} \mathrm{Ker}\,(\beta_i') = \left(\bigcap_{i=1}^{k+1} \mathrm{Ker}\,(\beta_i)\right) \cap \mathrm{Ker}\,(\beta_{k+1}) \subset \mathrm{Ker}\,(\alpha) \cap \mathrm{Ker}\,(\beta_{k+1}) = \mathrm{Ker}\,(\alpha')$$

On peut donc appliquer l'hypothèse de récurrence : il existe $\lambda_1, \ldots, \lambda_k \in \mathbb{K}$ tels que $\alpha' = \sum_{i=1}^{k} \lambda_i \beta_i'$. Ceci signifie que $\alpha - \sum_{i=1}^{k} \lambda_i \beta_i$ s'annule sur $\mathrm{Ker}\,(\beta_{k+1})$, c'est-à-dire que $\mathrm{Ker}\left(\alpha - \sum_{i=1}^{k} \lambda_i \beta_i\right) \subset \mathrm{Ker}\,(\beta_{k+1})$. D'après l'initialisation, il existe λ_{k+1} tel que $\alpha - \sum_{i=1}^{k} \lambda_i \beta_i = \lambda_{k+1}\beta_{k+1}$ et $\alpha \in \mathrm{Vect}\,(\beta_1, \ldots, \beta_{k+1})$.

13) La preuve est élémentaire pas récurrence sur n.

Si $n = 2$, on a $\dfrac{D(a_1, a_2)}{D(a_2)} = \dfrac{a_1 a_2 + 1}{a_2} = a_1 + \dfrac{1}{a_2} = [a1, a2]$.

Soit $n \geq 2$ et supposons le résultat démontré au rang n. Pour $a_1, \ldots, a_{n+1} > 0$, on a en développant $D(a_1, \ldots, a_{n+1})$ par rapport à la première colonne :

$$D(a_1, \ldots, a_{n+1}) = a_1 D(a_2, \ldots, a_{n+1}) - \det \begin{pmatrix} -1 & 0 & 0 & \ldots & 0 \\ 1 & a_3 & -1 & \ddots & \vdots \\ 0 & 1 & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & -1 \\ 0 & \ldots & 0 & 1 & a_{n+1} \end{pmatrix} = a_1 D(a_2, \ldots, a_{n+1}) + D(a_3, \ldots, a_{n+1})$$

En appliquant l'hypothèse de récurrence à la suite $(a_2, \ldots a_{n+1})$, on obtient :

$$\frac{D(a_1, \ldots, a_{n+1})}{D(a_2, \ldots, a_{n+1})} = a_1 + \frac{D(a_3, \ldots, a_{n+1})}{D(a_2, \ldots, a_{n+1})} = a_1 + \frac{1}{[a_2, \ldots, a_{n+1}]} = [a_1, \ldots, a_{n+1}].$$

14) Montrons le résultat par récurrence sur n.

- Si $n = 1$, $f : \ x \longmapsto a_1 e^{b_1 x}$ ne s'annule pas car $a_1 \neq 0$;
- Soit $n \geq 1$ et supposons le résultat vrai au rang n. Soient $b_1, \ldots, b_{n+1}$ des réels deux à deux distincts, $a_1, \ldots, a_{n+1}$ des réels non tous nuls et $f : \ x \longmapsto \sum_{k=1}^{n+1} a_k e^{b_k x}$. L'application $g : \ x \longmapsto f(x) e^{-b_{n+1} x}$ est de classe C^1 avec :

  $$g' : \ x \longmapsto \sum_{k=1}^{n} (b_k - b_{n+1}) a_k e^{(b_k - b_{n+1})x}$$

  Par hypothèse de récurrence (les $b_k - b_{n+1}$ sont deux à deux distincts et les $(b_k - b_{n+1})a_k$ sont non tous nuls), g' s'annule au plus $n-1$ fois. Le théorème de Rolle prouve alors que g s'annule au plus n fois, donc f s'annule au plus n fois.

Preuves d'existence

15) Pour $\theta \in]-\pi/4, 0[\cup]0, \pi/4]$, la condition $a \sin\theta \cos\theta + b(\cos^2\theta - \sin^2\theta) = 0$ est équivalente à la condition $\mathrm{cotan}(2\theta) = -\dfrac{a}{2b}$. L'application $\theta \longmapsto \mathrm{cotan}(2\theta)$ réalise une bijection de $]-\pi/4, 0[$ sur $]0, +\infty[$ et de $]0, \pi/4]$ sur $]-\infty, 0]$. On en déduit l'existence et l'unicité de θ.

16) a) Soit $M = (x, y, z)$ un point de Σ_1. Il existe donc $t, \theta \in \mathbb{R}$ tels que $x = t + \cos\theta$, $y = -t + \sin\theta$ et $z = \sin(2\theta)$. On en déduit :

$$(x+y)^2 - 1 = (\sin\theta + \cos\theta)^2 - 1 = 2\sin\theta\cos\theta = \sin(2\theta) = z$$

donc $\Sigma_1 \subset \Sigma_2$.

b) L'inclusion inverse est fausse car si $(x, y, z) \in \Sigma_1$, on a nécessairement $z \in [-1, 1]$: ainsi $(1, 1, 3) \in \Sigma_2 \setminus \Sigma_1$. On peut cependant démontrer que $\Sigma_1 = \Sigma_2 \cap \mathbb{R}^2 \times [-1, 1]$.

Soit $M = (x, y, z) \in \Sigma_2$ tel que $-1 \leq z \leq 1$. Il existe $\alpha \in \mathbb{R}$ tel que $z = \sin(2\alpha)$. On a alors :

$$(\sin\alpha + \cos\alpha)^2 = 1 + \sin(2\alpha) = 1 + z = (x+y)^2$$

Si $\sin\alpha + \cos\alpha = x + y$, on pose $\theta = \alpha$ et $t = x - \cos\theta$; sinon, on a $\sin\alpha + \cos\alpha = -x - y$: on pose $\theta = \alpha + \pi$ et $t = x - \cos\theta$. Dans les deux cas, on a $M = M(t, \theta)$ et $M \in \Sigma_1$.

Ainsi, Σ_1 est l'intersection de la surface Σ_2 d'équation $z = (x+y)^2 - 1$ et de la « couche » d'équation $-1 \leq z \leq 1$.

17) a) Première méthode : notons A l'ensemble des applications croissantes de I dans $\mathbb{R}$. On sait que si $f \in E$, il existe $n \in \mathbb{N}$, $f_1, \ldots, f_n \in A$ et $\lambda_1, \ldots \lambda_n \in \mathbb{R}$ tels que $f = \sum_{i=1}^{n} \lambda_i f_i$. En notant $I_+ = \{i \in [\![1, n]\!],\ \lambda_i \geq 0\}$ et $I_- = \{i \in [\![1, n]\!],\ \lambda_i < 0\}$, nous avons $f = \underbrace{\sum_{i \in I_+} \lambda_i f_i}_{=g} + \underbrace{\sum_{i \in I_-} \lambda_i f_i}_{=h}$, avec g croissante et h décroissante.

Réciproquement, si $f = g + h$ avec g croissante et h décroissante, on a $f = g - (-h) \in E$ car $g \in A$ et $-h \in A$.

Seconde méthode : notons $F = \{g + h,\ g, h :\ I \to \mathbb{R}\}$. On montre facilement que F est un s.e.v. de $\mathbb{R}^I$, que F contient A et que tout s.e.v. contenant A contient F :

- l'application nulle est élément de F (on choisit $g = h = 0$) ;
- si $f_1, f_2 \in F$, on peut écrire $f_1 = g_1 + h_1$ et $f_2 = g_2 + h_2$ avec g_1, g_2 croissantes et h_1, h_2 décroisantes. On a alors $f_1 + f_2 = (g_1 + g_2) + (h_1 + h_2) \in F$ car $g_1 + g_2$ est croissante et $h_1 + h_2$ décroisante ;
- si $f \in F$ et $\alpha \in \mathbb{R}$, on peut écrire $f = g + h$ avec g croissante et h décroissante ; si $\alpha \geq 0$, on a $\alpha f = (\alpha g) + (\alpha h) \in F$ car αg est croissante et αh est décroissante ; sinon, on a $\alpha f = \alpha h + \alpha g \in F$ car αh est croisante et αg est décroissante ;
- si $f \in A$, $f = f + 0 \in F$;
- si G est un s.e.v. contenant A et si $f = g + h$ avec g croissante et h décroissante, g et $-h$ sont éléments de A, donc de G, puis $f \in G$: on a donc $F \subset G$.

Ceci traduit que F est le s.e.v. engendré par A.

b) Soit $f \in F$: il existe g_0 et h_0 respectivement croissante et décroissante telles que $f = g_0 + h_0$. En posant $g = g_0 - g_0(\alpha)$ et $h = h + g_0(\alpha)$, on a toujours $f = g + h$, g croissante et h décroissante mais on a maintenant $g(\alpha) = 0$.

18) Dans ce cas très simple, on peut travailler par équivalence (mais ce n'est pas conseillé en général). Fixons F_0 une primitive de f. On sait que les primitives de f sont les fonctions de la forme $F_c = F_0 + c$ où c est une constante. Or nous avons :

$$\int_0^1 F_c(x)\,\mathrm{d}x = 0 \iff \int_0^1 F_0(x)\,\mathrm{d}x + c = 0 \iff c = -\int_0^1 F_0(x)\,\mathrm{d}x.$$

Le problème posé a donc une et une seule solution, qui est l'application $x \longmapsto F_0(x) - \displaystyle\int_0^1 F_0(t)\,\mathrm{d}t$.

19) Le plus simple est d'utiliser le théorème de définition des suites récurrentes : en notant $A = \mathbb{R}^+ \times \mathbb{R}$, l'application $f :\ (c, \lambda) \longmapsto \left(\sqrt{\dfrac{1+c}{2}}, \lambda\sqrt{\dfrac{2}{1+c}}\right)$ est définie de A dans lui-même ; on peut donc définir la suite $(c_n, \lambda_n)_{n\geq 1}$ en posant $(c_1, \lambda_1) = (0, 2)$ et $\forall n \in \mathbb{N}^*,\ (c_{n+1}, \lambda_{n+1}) = f(c_n, \lambda_n)$.

20) Notation : nous rappelons que pour $x \in K$ et $n \in \mathbb{Z}$, nous définissons nx de la façon suivante :

- si $n = 0$, $nx = 0$;
- pour tout $n \in \mathbb{N}$, $(n+1)x = nx + x$;
- pour tout $n \in \mathbb{N}$, $(-n)x = -(nx)$.

On montre facilement que pour tous $n, m \in \mathbb{Z}$ et pour tout $x \in K$, $(n+m)x = nx + mx$.

a) **Analyse :** supposons qu'un tel morphisme φ existe.

Nous avons $\varphi(1) = 1_K$, puis $\varphi(n) = \varphi(\underbrace{1 + \cdots + 1}_{n\text{fois}}) = \underbrace{\varphi(1) + \cdots + \varphi(1)}_{n\text{fois}} = n1_K$ pour tout $n \in \mathbb{N}$ (par récurrence sur n). On en déduit ensuite que $\varphi(-n) = -\varphi(n) = -(n1_K) = (-n)1_K$, toujours pour tout $n \in \mathbb{N}$. Ainsi, nous avons $\varphi(n) = n\,1_K$ pour tout $n \in \mathbb{Z}$. Ceci prouve l'unicité de φ.

Synthèse : l'application φ, qui à $n \in \mathbb{Z}$ associe $n1_K \in \mathbb{K}$ est un morphisme d'anneau :

- $\varphi(1) = 1_K$;
- $\forall n, m \in \mathbb{Z}$, $\varphi(n+m) = (n+m)1_K = n1_K + m1_K = \varphi(n) + \varphi(m)$;
- la propriété : $\forall n \in \mathbb{Z},\ \forall m \in \mathbb{N}$, $\varphi(nm) = \varphi(n)\varphi(m)$ se prouve trivialement par récurrence sur m ;
- $\forall n \in \mathbb{Z},\ \forall m \in \mathbb{N}$, $\varphi(n(-m)) = \varphi(-nm) = -\varphi(nm) = -\varphi(n)\varphi(m) = \varphi(n)\varphi(-m)$.

b) On suppose que $c = 0$.

Analyse : supposons que $\widetilde{\varphi}$ est un prolongement de φ en un morphisme d'anneau de $\mathbb{Q}$ dans K. Nous avons, pour $(p, q) \in \mathbb{Z} \times \mathbb{Z}^*$:

$$\varphi(p) = \widetilde{\varphi}\left(q\,\frac{p}{q}\right) = \widetilde{\varphi}(q)\widetilde{\varphi}\left(\frac{p}{q}\right) = \varphi(q)\widetilde{\varphi}\left(\frac{p}{q}\right)$$

donc $\widetilde{\varphi}(p/q) = \varphi(p)\left(\varphi(q)\right)^{-1}$: ceci prouve l'unicité de $\widetilde{\varphi}$.

Synthèse : nous pouvons définir l'application $\begin{array}{rccc} \widetilde{\varphi} : & \mathbb{Q} & \longrightarrow & K \\ & p/q & \longmapsto & \varphi(p)(\varphi(q))^{-1} \end{array}$. En effet, il suffit de vérifier la cohérence de cette définition :

- si $(p, q) \in \mathbb{Z} \times \mathbb{Z}^*$, $\varphi(p)(\varphi(q))^{-1}$ est bien défini car, φ étant injective, $\varphi(q)$ est un élément non nul de K ;
- si $p/q = p'/q'$ avec $p, p' \in \mathbb{Z}$ et $q, q' \in \mathbb{Z}^*$, on a $pq' = p'q$, donc $\varphi(p)\varphi(q') = \varphi(p')\varphi(q)$, puis $\varphi(p)(\varphi(q))^{-1} = \varphi(p')(\varphi(q'))^{-1}$

en remarquant que tous les éléments manipulés ici commutent ($\varphi(p)$ et $\varphi(q)$ commutent car $\varphi(p)\varphi(q) = \varphi(pq) = \varphi(qp) = \varphi(q)\varphi(p)$, puis en divisant à gauche et à droite $\varphi(q)$, $(\varphi(q))^{-1}\varphi(p) = \varphi(p)(\varphi(q))^{-1}$).

Il reste à vérifier que cette application est solution du problème :

- si $p \in \mathbb{Z}$, $\widetilde{\varphi}(p) = \varphi(p)(\varphi(1))^{-1} = \varphi(p)(1_K)^{-1} = \varphi(p)$ donc $\widetilde{\varphi}$ est un prolongement de φ ;
- $\widetilde{\varphi}(1) = \varphi(1) = 1_K$;

- pour $x = \dfrac{p}{q} et x' = \dfrac{p'}{q'}$ éléments de $\mathbb{Q}$, nous avons, en utilisant une nouvelle fois la commutativité :

$$\begin{aligned}
\widetilde{\varphi}(x+x') &= \widetilde{\varphi}\left(\frac{pq'+p'q}{qq'}\right) = \varphi(pq'+p'q)\left(\varphi(qq')\right)^{-1} \\
&= \left(\varphi(p)\varphi(q')+\varphi(p')\varphi(q)\right)\varphi(q')^{-1}\varphi(q)^{-1} = \varphi(p)(\varphi(q))^{-1}+\varphi(p')\left(\varphi(q')\right)^{-1} \\
&= \widetilde{\varphi}(x)+\widetilde{\varphi}(x')
\end{aligned}$$

$$\begin{aligned}
\widetilde{\varphi}(xx') &= \widetilde{\varphi}\left(\frac{pp'}{qq'}\right) \\
&= \varphi(pp')\left(\varphi(qq')\right)^{-1} = \varphi(p)\varphi(p')(\varphi(q'))^{-1}(\varphi(q))^{-1} \\
&= \widetilde{\varphi}(x)\widetilde{\varphi}(x')
\end{aligned}$$

$\widetilde{\varphi}$ est ainsi le seul morphisme d'anneau de $\mathbb{Q}$ dans K qui prolonge φ. Ce morphisme est injectif, car :

$$p/q \in \mathrm{Ker}\,(\widetilde{\varphi}) \Longleftrightarrow \varphi(p)(\varphi(q))^{-1} = 0 \Longleftrightarrow \varphi(p) = 0 \Longleftrightarrow p = 0 \Longleftrightarrow p/q = 0.$$

L'image de $\widetilde{\varphi}$ est donc un sous-anneau de K isomorphe à $\mathbb{Q}$; ce sous-anneau est donc un corps. C'est le plus petit sous-corps de K (appelé sous-corps premier de K). Ainsi, on a « plongé » $\mathbb{Q}$ dans K et on peut dire que $\mathbb{Q}$ est un sous-corps de K.

c) **Analyse :** si un tel morphisme $\widetilde{\varphi}$ existe, nous avons $\widetilde{\varphi}(\overline{1}) = 1_K$ puis, pour tout entier $n \in \mathbb{Z}$, $\widetilde{\varphi}(\overline{n}) = \widetilde{\varphi}(n\,\overline{1}) = n1_K = \varphi(n)$, d'où l'unicité de $\widetilde{\varphi}$.

Synthèse : l'application $\begin{array}{ccc} \mathbb{Z}/c\mathbb{Z} & \longrightarrow & K \\ \overline{n} & \longmapsto & \varphi(n) \end{array}$ est bien définie, car pour $n, m \in \mathbb{Z}$ tels que $\overline{n} = \overline{m}$, on a $n - m \in c\mathbb{Z} = \mathrm{Ker}\,(\varphi)$, donc $\varphi(n) = \varphi(m)$. On vérifie ensuite facilement que $\widetilde{\varphi}$ est un morphisme d'anneau :

- $\widetilde{\varphi}(\overline{1}) = \varphi(1) = 1_K$;
- $\forall n, m \in \mathbb{Z},\ \widetilde{\varphi}(\overline{n}+\overline{m}) = \widetilde{\varphi}(\overline{n+m}) = \varphi(n+m) = \varphi(n)+\varphi(m) = \widetilde{\varphi}(\overline{n})+\widetilde{\varphi}(\overline{m})$;
- $\forall n, m \in \mathbb{Z},\ \widetilde{\varphi}(\overline{n}\,\overline{m}) = \widetilde{\varphi}(\overline{nm}) = \varphi(nm) = \varphi(n)\varphi(m) = \widetilde{\varphi}(\overline{n})\,\widetilde{\varphi}(\overline{m})$.

On a cette fois :

$$\forall n \in \mathbb{Z},\ \overline{n} \in \mathrm{Ker}\,(\widetilde{\varphi}) \Longleftrightarrow \varphi(n) = 0 \Longleftrightarrow n \in \mathrm{Ker}\,(\varphi) \Longleftrightarrow n \in c\mathbb{Z} \Longleftrightarrow \overline{n} = \overline{0}$$

donc $\widetilde{\varphi}$ est injective.

On en déduit que $\widetilde{\varphi}$ est un isomorphisme de $\mathbb{Z}/c\mathbb{Z}$ sur $\mathrm{Im}\,(\widetilde{\varphi})$, qui est un sous-anneau de K ; comme K est intègre, $\mathrm{Im}\,(\widetilde{\varphi})$ l'est également, ce qui prouve que $\mathbb{Z}/c\mathbb{Z}$ est intègre : c est donc un nombre premier. On en déduit que $\mathbb{Z}/c\mathbb{Z}$ est un corps, puis que $\mathrm{Im}\,(\widetilde{\varphi})$ en est également un : c'est le sous-corps premier de K.

Conclusion : dans cet exercice, nous avons démontré que tout corps K est soit un sur-corps de $\mathbb{Q}$, soit un sur-corps d'un corps fini $\mathbb{Z}/p\mathbb{Z}$. Dans le premier cas, on dit que K est de caractéristique nulle ; dans le second cas, K est de caractéristique p.

Exercices divers

21) Pour définir une telle surjection f, on peut choisir $i_1 < i_2$ dans $\{1, 2, \ldots, n+1\}$, choisir une permutation de $\{1, 2, \ldots, n\}$ et définir :

$$\forall i \in \{1, 2, \ldots, n+1\},\ f(i) = \begin{cases} \sigma(i) & \text{si } 1 \leq i < i_2 \\ \sigma(i_1) & \text{si } i = i_2 \\ \sigma(i-1) & \text{si } i_2 < i \leq n+1 \end{cases}$$

Chaque surjection est ainsi construite une et une seule fois : il existe donc $\binom{n+1}{2} n! = \frac{n}{2}(n+1)!$ surjections de $\{1,2,\dots,n+1\}$ sur $\{1,2,\dots,n\}$.

22) a) L'identité est une bijection de A sur lui-même.

b) Si φ est une bijection de A sur B, φ^{-1} est une bijection de B sur A.

c) Si φ_1 et φ_2 sont des bijections de A sur B et de B sur C, $\varphi_2 \circ \varphi_1$ est une bijection de A sur C.

d) Si φ est une bijection de A sur B, l'application $\Phi : \mathcal{P}(A) \longrightarrow \mathcal{P}(B)$ définie par :

$$\forall E \subset A,\ \Phi(E) = \{\varphi(x),\ x \in E\}$$

est une bijection de $\mathcal{P}(A)$ sur $\mathcal{P}(B)$. Dans la pratique, on utilise l'abus d'écriture $\Phi(E) = \varphi(E)$.

e) Pour $f : A \times B \longrightarrow C$, on note F l'application de B dans C^A définie par :

$$\forall (x,y) \in A \times B,\ F(y)(x) = f(x,y).$$

L'application $f \longmapsto F$ est une bijection de $C^{A\times B}$ sur $\left(C^A\right)^B$.

f) Si φ_1 et φ_2 sont des bijections de A sur C et de B sur D, les applications $(x,y) \longmapsto (\varphi_1(x), \varphi_2(x))$ et $f \longmapsto \varphi_1 \circ f \circ \varphi_2^{-1}$ sont des bijections respectivement de $A \times B$ sur $C \times D$ et de A^B sur C^D.

23) Un élément $n \geq 2$ est minimal si et seulement si :

$$\forall m \geq 2,\ m \,|\, n \Longrightarrow m = n$$

ce qui est la définition d'un nombre premier.

24) Notons $A = \bigcup_{n\geq 0} A_n$ et $B = \bigcup_{n\geq 1} B_n$.

On peut commencer par remarquer que la définition de φ est cohérente, car si $x \notin A$, $x \notin A_0$ et donc $x \in g(F)$: x possède donc un unique antécédent par g, que nous notons $g^{-1}(x)$.

Injectivité : supposons que x_1 et x_2 sont deux éléments de E vérifiant $\varphi(x_1) = \varphi(x_2)$. Nous sommes dans l'un des cas suivant :

- x_1 et x_2 sont éléments de A : on a alors $f(x_1) = f(x_2)$, donc $x_1 = x_2$ car f est injective ;
- un seul des deux éléments (par exemple x_1) est élément de A : on a alors $f(x_1) = g^{-1}(x_2)$, soit $x_2 = g \circ f(x_1)$, ce qui n'est pas possible, puisque $g \circ f(x_1) \in \bigcup_{n\geq 1} A_n \subset A$ et $x_2 \notin A$;
- ni x_1, ni x_2 n'appartiennent à A : on a alors $g^{-1}(x_1) = g^{-1}(x_2)$, d'où $x_1 = x_2$.

Ainsi, dans tous les cas, $x_1 = x_2$ et φ est injective.

Surjectivité : soit $y \in F$. On cherche à montrer qu'il existe $x \in E$ tel que $\varphi(x) = y$. Procédons par analyse, en supposant qu'un tel x existe. Deux cas sont alors possibles :

- si $x \in A$, $y = f(x)$ et donc $x = f^{-1}(y)$;
- sinon, $y = g^{-1}(x)$ et donc $x = g(y)$.

La synthèse va donc se faire par disjonction de cas, mais il faut remplacer la disjonction sur x de l'analyse par une disjonction sur y. On peut deviner que c'est l'appartenance de y à B qui va correspondre à l'appartenance de x à A (mais on pourrait aussi prolonger la synthèse pour montrer que dans le cas $x \in A$ (resp. $x \notin A$), on a bien $y \in B$ (resp. $y \notin B$)).

- Si $y \in B$, il existe $n \geq 1$ tel que $y \in B_n = f(A_{n-1})$. Ainsi, il existe un $x \in A_{n-1}$ tel que $y = f(x)$: on a bien $x \in A$ et $\varphi(x) = y$.

- Sinon, posons $x = g(y)$. Par définition, $x \notin A_0$ (car $x \in g(F)$) et s'il existait $n \geq 1$ tel que $x \in A_n$, il existerait $y' \in B_{n-1}$ tel que $x = g(y')$, ce qui imposerait $y = y' \in B$ (car g est injective) : ce serait absurde. Nous avons donc prouvé que $x \notin A$, ce qui permet d'affirmer que $\varphi(x) = g^{-1}(x) = y$.

Dans tous les cas, y possède un antécédent par φ, qui est donc surjective.

25) supposons que $A \in f(E)$. Il existe alors $x_0 \in E$ tel que $f(x_0) = A$. Nous devons donc utiliser l'élément x_0 de E et la partie A de E pour exhiber une absurdité ... la seule question naturelle qui se pose quand on a un élément x_0 et une partie A d'un ensemble E est l'appartenance éventuelle de x_0 à A. Nous avons ici :

$$x_0 \in A \Longleftrightarrow x_0 \notin f(x_0) \Longleftrightarrow x_0 \notin A$$

ce qui est bien absurde. Nous avons ainsi montré par une preuve par l'absurde que A n'était pas dans l'image de f. Autrement-dit, il n'existe pas de surjection de E sur $\mathcal{P}(E)$. Comme il existe une injection de E dans $\mathcal{P}(E)$, on peut donc dire que le cardinal de $\mathcal{P}(E)$ est strictement plus grand que celui de E.

Cette propriété prouve que l'on ne peut pas parler de l'ensemble de tous les ensembles. En effet, si un tel ensemble E pouvait être défini, alors $\mathcal{P}(E)$ serait contenu dans E (puisqu'une partie de E est un ensemble). Nous pourrions alors définir $\varphi :\ E \longrightarrow \mathcal{P}(E)$ par :

$$\forall A \in E,\ \varphi(A) = \begin{cases} A & \text{si } A \in \mathcal{P}(E) \\ \emptyset & \text{sinon} \end{cases}$$

qui serait une surjection de E sur $\mathcal{P}(E)$.

26) Si E et F sont deux ensembles, nous noterons $E \sim F$ la propriété "il existe une bijection de E et F" (on dit alors que E et F sont équipotent, ou qu'ils ont même *potentiel*, ou même *cardinal*).

a) La numérotation $\mathbb{Z} = \{0, -1, 1, -2, 2, -3, 3, \ldots\}$ de $\mathbb{Z}$ donne une bijection φ de $\mathbb{N}$ sur $\mathbb{Z}$. On peut aussi écrire une définition formelle :

$$\forall n \in \mathbb{N},\ \varphi(n) = \begin{cases} \dfrac{n}{2} & \text{si } n \text{ est pair} \\ -\dfrac{n+1}{2} & \text{sinon} \end{cases}$$

mais le caractère bijectif de φ ne saute plus aux yeux.

b) On peut numéroter $\mathbb{N}^2$ en diagonal :

$$\mathbb{N}^2 = \{(0,0), (1,0), (0,1), (2,0), (1,1)(0,2), (3,0), (2,1), (1,2), (0,3), \ldots\}$$

Pour être plus précis, on peut remarquer que $\mathbb{N}^2$ est la réunion disjointe des parties

$$\forall n \in \mathbb{N},\ E_n = \{(x,y) \in \mathbb{N}^2,\ x + y = n\}$$

Comme les E_n sont finies et non vides, $\mathbb{N}^2$ est dénombrable.

Les amateurs de "formules" peuvent vérifier que l'application :

$$\varphi :\ (i,j) \longmapsto \frac{(i+j)(i+j+1)}{2} + j$$

est une bijection de $\mathbb{N}^2$ sur $\mathbb{N}$, qui correspond à la numérotation précédente : le point (i,j) est sur la diagonale d'équation $D_{i+j} :\ x + y = i + j$. Il faut donc compter le nombre de points présents sur les diagonales D_0, D_1, ..., D_{i+j-1}, soient $1+2+\cdots+(i+j) = \dfrac{(i+j)(i+j+1)}{2}$ points, et ajouter les j points $(0, i+j), (1, i+j-1), \ldots, (i+1, j-1)$ pour atteindre (i,j), qui aura donc le "numéro" $(i+j)(i+j+1)2 + j$.

Grâce à ce résultat, on montre qu'une réunion dénombrable d'ensembles dénombrables est dénombrable, c'est-à-dire que si I est un ensemble dénombrable et si pour tout $i \in I$, E_i est un ensemble dénombrable, alors $E = \bigcup_{i \in I} E_i$ est également dénombrable. En effet, en notant, pour tout $i \in I$,φ_i une bijection de $\mathbb{N}$ sur E_i, l'application qui à (i,j) associe $\varphi_i(j)$ est une surjection de $\mathbb{N}^2$ dans E, qui est donc au plus dénombrable. Comme $E_1 \subset E$, E est infini : il est donc dénombrable.

c1) On peut une nouvelle fois numéroter les rationnels :

$$\mathbb{Q} = \{0, 1, -1, 2, \frac{3}{2}, \frac{1}{2}, -\frac{1}{2}, -\frac{3}{2}, -2, 3, \frac{8}{3}, \frac{5}{2}, \frac{7}{3}, \frac{5}{3}, \frac{4}{3}, \frac{2}{3}, \frac{1}{3}, -\frac{1}{3}, -\frac{2}{3}, -\frac{4}{3}, -\frac{5}{3}, -\frac{7}{3}, -\frac{5}{2}, -\frac{8}{3}, -3, \ldots\}$$

L'idée est de balayer les rationnels de n à $-n$ en plaçant tous les rationnels non encore rencontrés dont le dénominateur est inférieur ou égal à n. Nous serions évidemment incapable de donner une formule pour la bijection précédente.

c2) Plus rigoureusement : pour $n \in \mathbb{N}^*$, on note E_n l'ensemble des rationnels de $[-n, n]$ qui s'écrivent $\frac{a}{b}$ avec $1 \leq b \leq n$. Chaque partie E_n est finie et $\mathbb{Q} = \bigcup_{n\geq 1} E_n$: $\mathbb{Q}$ est donc fini ou dénombrable ... donc dénombrable.

c3) En utilisant Cantor-Bernstein : pour $r \in \mathbb{Q}$, on peut écrire "canoniquement" $r = \dfrac{p}{q}$ avec $p = 0, q = 1$ si $r = 0$ et $p \in \mathbb{Z}$, $q \in \mathbb{N}$ et $p \wedge q = 1$ si $r \neq 0$. Les deux applications :

$$\begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{Q} \\ n & \longmapsto & n \end{array} \quad \text{et} \quad \begin{array}{ccc} \mathbb{Q} & \longrightarrow & \mathbb{Z} \times \mathbb{N} \\ r & \longmapsto & (p, q) \end{array}$$

sont alors injectives. Comme $\mathbb{Z} \times \mathbb{N}$ est dénombrable, i.e. en bijection avec $\mathbb{N}$, nous avons construit une injection de $\mathbb{N}$ dans $\mathbb{Q}$ et une injection de $\mathbb{Q}$ dans $\mathbb{N}$: les deux ensembles sont en équipotents.

d) Nous allons une nouvelle fois utiliser Cantor-Bernstein. Remarquons pour commencer que $\mathbb{R}$ est équipotent à $]0, 1[$ (utiliser une bijection type Arctan) et que $[0, 1[$ est équipotent à $]0, 1[$ (on construit très facilement deux injections). Nous avons ensuite :

- $(a_n)_{n\in\mathbb{N}} \longmapsto \displaystyle\sum_{n=0}^{+\infty} a_n 10^{-n-1}$ est une injection de $\{0, 1\}^{\mathbb{N}}$ dans $[0, 1[$;
- $x \longmapsto (a_n)_{n\in\mathbb{N}}$ où $x = 0, a_0a_1a_2\ldots$ est l'écriture propre de x en base 2 est une injection de $[0, 1[$ dans $\{0, 1\}^{\mathbb{N}}$.

On en déduit que $\mathbb{R} \sim [0, 1[\sim \{0, 1\}^{\mathbb{N}}$.

e) On a ensuite :

$$\mathbb{R}^2 \sim \{0, 1\}^{\mathbb{N}} \times \{0, 1\}^{\mathbb{N}} \sim \{0, 1\}^{\mathbb{N}}$$

puisque l'application $((x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}}) \longmapsto (x_0, y_0, x_1, y_2, x_2, y_2, \ldots)$ est une bijection de $\{0, 1\}^{\mathbb{N}} \times \{0, 1\}^{\mathbb{N}}$ sur $\{0, 1\}^{\mathbb{N}}$.

f) De même :

$$\mathbb{R}^{\mathbb{N}} \sim \left(\{0, 1\}^{\mathbb{N}}\right)^{\mathbb{N}} \sim \{0, 1\}^{\mathbb{N}^2} \sim \{0, 1\}^{\mathbb{N}}$$

g) $\mathcal{P}(\mathbb{N})$ est équipotent à $\{0, 1\}^{\mathbb{N}}$ (on associe à une partie de $\mathbb{N}$ sa fonction indicatrice), donc $\mathbb{R}$ n'est pas dénombrable (aucun ensemble E n'est équipotent à $\mathcal{P}(E)$).

La preuve de la non dénombrabilité de $\mathbb{R}$ peut se faire directement : si φ est une application de $\mathbb{N}$ dans $\mathbb{R}$, on peut écrire, pour tout $n \in \mathbb{N}$, l'écriture décimale :

$$\varphi(n) = E_n + 0, a_{n,0}a_{n,1}a_{n,2}\ldots$$

où E_n est la partie entière de $\varphi(n)$ et $(a_{n,i})_{i\geq 0}$ est une suite de $\{0, 1, \ldots, 9\}$ non stationnaire à la valeur 9. Pour chaque $n \in \mathbb{N}$, on peut fixer $b_n \in \{0, 1, \ldots, 8\}$ distinct de $a_{n,n}$. L'écriture décimale $0, b_0b_1b_2\ldots$ est alors l'écriture propre (les b_n ne stationnent pas à la valeur 9) d'un réel y qui est distinct de chaque $\varphi(n)$ (leurs écritures décimales diffère pour au moins une décimale) : l'application φ n'est donc pas surjective, ce qui prouve que $\mathbb{R}$ n'est pas dénombrable.

27) En utilisant Cantor-Bernstein : pour $r \in \mathbb{Q}$, on peut écrire "canoniquement" $r = \dfrac{p}{q}$ avec $p = 0, q = 1$ si $r = 0$ et $p \in \mathbb{Z}$, $q \in \mathbb{N}$ et $p \wedge q = 1$ si $r \neq 0$. Les deux applications :

$$\begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{Q} \\ n & \longmapsto & n \end{array} \quad \text{et} \quad \begin{array}{ccc} \mathbb{Q} & \longrightarrow & \mathbb{Z} \times \mathbb{N} \\ r & \longmapsto & (p, q) \end{array}$$

sont alors injectives. Comme $\mathbb{Z} \times \mathbb{N}$ est dénombrable, i.e. en bijection avec $\mathbb{N}$, nous avons construit une injection de $\mathbb{N}$ dans $\mathbb{Q}$ et une injection de $\mathbb{Q}$ dans $\mathbb{N}$: les deux ensembles sont en équipotents.

Pour $n \in \mathbb{N}$, notons E_n l'ensemble des polynômes rationnels de degré n. Nous avons alors :

$$\mathbb{Q}[X] = \{0\} \sqcup E_0 \sqcup E_1 \sqcup E_2 \sqcup \dots$$

Or pour $n \geq 0$, $E_n \sim \mathbb{Q}^n \times \mathbb{Q}^*$. Comme $\mathbb{Q}^* \sim \mathbb{N}$, nous avons donc $E_n \sim \mathbb{Q}^{n+1} \sim \mathbb{N}$ et donc $\mathbb{Q}[X]$ est une réunion dénombrable d'ensemble dénombrable, il est donc dénombrable.

En écrivant $\mathbb{Q}[X] = \{P_n,\ n \in \mathbb{N}\}$, notons A_n l'ensemble des racines réelles de P_n. L'ensemble des réels algébriques est donc $A = \bigcup_{n\in\mathbb{N}} A_n$, qui est une réunion dénombrable d'ensembles finis : il est donc au plus dénombrable, donc dénombrable (A contient $\mathbb{Q}$).

Comme A est dénombrable et $\mathbb{R}$ ne l'est pas, sil existe au moins un réel transcendant. On peut même dire beaucoup mieux : l'ensemble T des nombres transcendants n'est pas dénombrable (sinon, $\mathbb{R} = A \cup T$ le serait). On peut aller encore un peu plus loin et démontrer que T et $\mathbb{R}$ ont même cardinal (on dit que T a la *puissance du continu*). En effet, comme T est infini, on peut écrire $T = T_0 \sqcup T_1 \sqcup T_2$ avec T_1 et T_2 dénombrable. On a alors :

$$T = T_0 \sqcup T_1 \sqcup T_2 \sim T_0 \sqcup \mathbb{N}$$

puisque $T_1 \sqcup T_2$ est dénombrable. On a ensuite :

$$T = T_0 \sqcup \mathbb{N} \sqcup A \sim T \sqcup A = \mathbb{R}$$

puisque $T_1 \sim \mathbb{N}$ et $T_2 \sim \mathbb{N} \sim A$.

Remarque : nous avons ici une preuve d'existence non constructive, puisque nous n'avons mis en évidence aucun nombre transcendant, tout en ayant démontré que presque tous les réels sont transcendants.

28) Considérons les écritures décimales des x_n :

$$\forall n \in \mathbb{N},\ x_n = E_n + 0, a_{n,0}a_{n,1}a_{n,2}\dots$$

où E_n est la partie entière de x_n et $(a_{n,i})_{i\geq 0}$ est une suite de $\{0, 1, \dots, 9\}$ non stationnaire à la valeur 9. Pour chaque $n \in \mathbb{N}$, on peut fixer $b_n \in \{0, 1, \dots, 8\}$ distinct de $a_{n,n}$. L'écriture décimale $0, b_0b_1b_2\dots$ est alors l'écriture propre (les b_n ne stationnent pas à la valeur 9) d'un réel y qui est distinct de chaque x_n (les écritures décimales de y et de x_n on au moins une décimale qui diffère) : y n'est donc pas élément de D, ce qui prouve que $\mathbb{R}$ n'est pas dénombrable.

29) L'inégalité de Cauchy-Schwarz donne, pour $\sigma \in S_n$:

$$\sum_{k=1}^{n} k\sigma(k) \leq \sqrt{\sum_{k=1}^{n} k^2} \times \sqrt{\sum_{k=1}^{n} \sigma(k)^2} = \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6} = M_n.$$

On a un cas d'égalité pour $\sigma = Id$ (et uniquement dans ce cas là, d'après l'étude du cas d'égalité dans l'inégalité de Cauchy-Schwarz), donc le maximum cherché est égal à M_n.

Nous allons utiliser une petite astuce pour ramener le calcul du minimum à celui du maximum. Notons τ la permutation $k \longmapsto n+1-k$. L'application $\sigma \longmapsto \sigma' = \tau \circ \sigma$ est une bijection de S_n sur lui-même, donc :

$$m_n = \min_{\sigma\in S_n} \sum_{k=1}^{n} k\sigma(k) = \min_{\sigma\in S_n} \sum_{k=1}^{n} k\sigma'(k) = \min_{\sigma\in S_n} \sum_{k=1}^{n} k(n+1-\sigma(k)) = \min_{\sigma\in S_n} \left(\underbrace{\sum_{k=1}^{n} k(n+1)}_{=n(n+1)^2/2} - \sum_{k=1}^{n} k\sigma(k) \right).$$

Comme le minimum de l'opposé est l'opposé du maximum, nous obtenons :

$$m_n = \frac{n(n+1)^2}{2} - M_n = \frac{n(n+1)(n+2)}{6}$$

et ce minimum est atteint quand $\sigma = \tau$ (et uniquement dans ce cas là).

30) a) Soit A une partie non vide de $E_1 + E_2$. Si $A \subset E_2$, A possède un plus petit élément m dans l'ensemble bien ordonné $(E_2, \leq_2)$. Sinon, $A \cap E_1$ est une partie non vide de E_1, qui possède donc un plus petit élément m dans l'ensemble bien ordonné $(E_1, \leq_1)$. Dans les deux cas, m le plus petit élément de A dans $(E, \leq)$.

Si $E_1 = \{a\}$ est un singleton et si $E_2 = \mathbb{N}$ (avec leurs bons ordres canoniques), $E_1 + E_2$ n'est pas isomorphe à $E_2 + E_1$ ($E_1 + E_2$ n'a pas de plus grand élément alors que a est le maximum de $E_2 + E_1$).

b) Notons $\leq$ l'ordre lexicographique. Soit A une partie non vide de $E_1 \times E_2$. Notons $A_1 = \{x_1 \in E_1,\ \exists\, x_2 \in E_2,\ (x_1, x_2) \in A\}$. A_1 est une partie non vide de E_1, donc elle possède un plus petit élément m_1. Notons ensuite $A_2 = \{x_2 \in E_2,\ (m_1, x_2) \in A\}$. A_2 est une partie non vide de E_2 (car $m_1 \in A_1$), donc elle possède un plus petit élément m_2. Si (x_1, x_2) appartient à A, on a :

- $x_1 \in A_1$, donc $m_1 \leq_1 x_1$;
- si $m_1 <_1 x_1$, on a bien $(m_1, m_2) \leq (x_1, x_2)$;
- sinon, $m_1 = x_1$ et $x_2 \in A_2$, donc $m_2 \leq_2 x_2$ et $(m_1, m_2) \leq (x_1, x_2)$.

A possède donc un plus petit élément : $E_1 \times E_2$ est bien ordonné par l'ordre lexicographique.

Notons $E_1 = \{0, 1\}$ et $E_2 = \mathbb{N}$ muni de leurs (bons) ordres canoniques. $E_2 \times E_1$ est isomorphe à $\mathbb{N}$ alors que $E_1 \times E_2$ ne l'est pas (la partie $\{(0, n),\ n \in \mathbb{N}\} \subset E_1 \times E_2$ est infinie et majorée par $(1, 0)$, mais $\mathbb{N}$ ne contient pas de partie infinie majorée). On peut se représenter ces deux ensemble de la façon suivantes :

$$E_1 \times E_2 :\ (0,0) < (0,1) < (0,2) < \cdots < (1,0) < (1,1) < (1,2) \ldots$$

$$E_2 \times E_1 :\ (0,0) < (0,1) < (1,0) < (1,1) < (2,0) < (2,1) < \ldots$$

Remarque : un ensemble bien ordonné représente un *ordinal* (deux ensembles bien ordonnés représentent le même ordinal si et seulement s'ils sont isomorphes). Les premiers ordinaux sont les nombres entiers, n désignant l'ensemble $\{0, 1, \ldots, n-1\}$ muni de son bon ordre usuel. Le premier ordinal infini est représenté par $(\mathbb{N}, \leq)$: on le note ω. Nous venons de définir une arithmétique (i.e. une somme et un produit) sur les ordinaux. Dans cette arithmétique, nous avons par exemple $2 + 3 = 3 + 2 = 5$, $2 \times 3 = 3 \times 2 = 6$, $1 + \omega = \omega \neq \omega + 1$ et pour tout ordinal α, $0 + \alpha = \alpha + 0 = \alpha$ et $1 \times \alpha = \alpha \times 1 = \alpha$.

Exercices X-ENS

31) Soit φ qui, à $x \in X$, associe le nombre d'indices i tels que $x \in X_i$. Nous avons clairement :

$$\forall x \in X,\ x \in Y_k \iff \varphi(x) \geq k.$$

L'idée, pour travailler sur Z_k, est simplement de passer au complémentaire :

$$\forall x \in X,\ x \notin Z_k \iff \exists I \in \mathcal{P}_k,\ \forall i \in I,\ x \notin X_i \iff \varphi(x) \leq n - k$$

ce qui donne :

$$\forall x \in X,\ x \in Z_k \iff \varphi(x) \geq n - k + 1.$$

On en déduit donc que $Y_k \subset Z_k$ si $2k \geq n + 1$ et $Z_k \subset Y_k$ si $n + 1 \leq 2k$.

En particulier, $Y_k = Z_k$ quand $n + 1 = 2k$.

32) Fixons $a \in E$ (E est non vide). Nous pouvons définir la suite $(a^n)_{n \geq 1}$ par récurrence :

$$\begin{cases} a^1 = a \\ \forall n \in \mathbb{N}^*,\ a^{n+1} = a^n * a \end{cases}$$

et l'associativité de $*$ donne :

$$\forall n, p \in \mathbb{N}^2 \setminus \{(0,0)\},\ a^n * a^p = a^{n+p}.$$

Comme E est fini, il existe deux entiers naturels n et m tels que $n < m$ et $a^{2^n} = a^{2^m}$. Nous avons alors :

$$\forall p \in \mathbb{N}, a^{2^n+p} = a^{2^m+p}$$

et l'idée consiste à chercher une valeur de p telle que $2(2^n + p) = 2^m + p$. Il suffit donc de poser $p = 2^m - 2^{n+1}$, qui est bien élément de $\mathbb{N}$ puisque $m \geq n + 1$, puis $e = a^{2^m+p}$ pour obtenir $e * e = e$.

33) Si $E = \{x_1, x_2, \ldots, x_n\}$ est un ensemble fini et si f est l'application définie par $f(x_n) = x_0$ et $\forall 1 \leq i \leq n-1$, $f(x_i) = x_{i+1}$, $\emptyset$ et A sont stables par f, et ce sont les seules parties stables. En effet, si $f(A) \subset A$ et si A est non vide, il existe i tel que $x_i \in A$: A contient alors les images successives de x_i par f, c'est-à-dire $x_{i+1}, \ldots, x_n, x_1, \ldots, x_{i-1}$ et $A = E$.

Supposons maintenant que E est infini et soit $f : E \longrightarrow E$. Soit x_0 un élément de E et définissons la suite $(x_n)_{n\geq 0}$ par $\forall n \in \mathbb{N},\ x_{n+1} = f(x_n)$.

Posons $A = \{x_n,\ n \geq 1\}$. A est clairement stable par f et non vide. Il reste à montrer que $A \neq E$, ce qui se fait par disjonction de cas :

- si $x_0 \notin A$, A n'est pas égal à E ;
- sinon, il existe $k \geq 1$ tel que $x_k = x_0$ et la suite $(x_n)_{n\geq 0}$ est périodique : A est alors fini et différent de E, qui est infini.

34) Les deux premiers cas sont possibles, avec $\sigma = Id$ ou $\sigma : n \longmapsto \begin{cases} n+1 & \text{si } n \text{ est pair} \\ n-1 & \text{sinon} \end{cases}$.

Le troisième cas ne peut se produire. Soit en effet la relation $\sim$ définie sur $\mathbb{N}$ par :

$$\forall\, n, m \in \mathbb{N},\ n \sim m \Longleftrightarrow \exists k \in \mathbb{Z},\ m = \sigma^k(n).$$

Cette relation est clairement une relation d'équivalence. Si n est un élément de $\mathbb{N}$, la classe de n pour $\sim$, notée $\overline{n}$, est une partie non vide de $\mathbb{N}$: son minimum m est alors élément de A, puisque $\sigma(m) \in \overline{n}$. Si l'ensemble quotient $\mathbb{N}/_\sim$ est infini, l'ensemble A est donc également infini, puisque l'application

$$\begin{array}{ccc} \mathbb{N}/_\sim & \longrightarrow & A \\ \theta & \longmapsto & \min\theta \end{array}$$

est injective. Sinon, il existe $n \in \mathbb{N}$ tel que $\overline{n}$ soit une partie infinie. Les éléments de la suite $(\sigma^p(n))_{p\in\mathbb{Z}}$ sont deux à deux distincts (sinon, cette suite serait périodique et $\overline{n}$ serait finie). Cette suite d'entiers naturels ne peut pas être strictement décroissante à partir d'un certain rang : il existe donc des entiers p arbitrairement grands tels que $\sigma^p(n) \leq \sigma^{p+1}(n)$. Il existe ainsi une infinité d'entiers p tels que $\sigma^p(n)$ soit élément de A et A est infini.

35) Les parties $E_i = \{i\}$, pour $1 \leq i \leq n$, vérifient les hypothèses demandées, donc le maximum cherché est au moins égal à n.

Supposons que $(E_i)_{\leq i\leq k}$ vérifie les hypothèses. Notons :

- pour $j \in \{1, 2, \ldots, k\}$, C_j le vecteur de $(\mathbb{Z}/2\mathbb{Z})^n$ dont la j-ème coordonnée vaut 1 si $j \in E_j$ et 0 sinon ;
- A la matrice de taille $n \times k$ de colonnes $(C_1, C_2, \ldots, C_k)$.

Cette définition est naturelle, car $\mathcal{P}(\{1, 2, \ldots, n\})$ s'identifie à $\{0, 1\}^{\{1,2,\ldots,n\}}$, et donc à $\{0, 1\}^n$.

L'hypothèse sur les cardinaux des E_i et $E_i \cap E_j$ s'écrit alors : ${}^tAA = I_k$. A étant une matrice de taille $n \times k$, on a alors :

$$k = \mathrm{rg}(I_k) = \mathrm{rg}({}^tAA) \leq \mathrm{rg}({}^tA) \leq \min(n, k) \leq n$$

ce qui prouve que la valeur $k = n$ est maximale. On peut aussi remarquer que $(E_i)_{1\leq i\leq k}$ vérifie les propriétés cherchée si et seulement $(C_1, C_2, \ldots, C_k)$ est une famille libre de $(\mathbb{Z}/2\mathbb{Z})^n$.

36) Pour tout réel a, les ensembles $A = \{q \in \mathbb{Q},\ q \leq a\}$ et $B = \{q \in \mathbb{Q},\ q > a\}$ sont infinis dénombrables : il existe donc une bijection φ de A sur B. Notons alors σ_a la permutation de $\mathbb{Q}$ définie par

$$\forall q \in \mathbb{Q},\ \sigma_a(q) = \begin{cases} \varphi(q) & \text{si } q \in A \\ \varphi^{-1}(q) & \text{si } q \in B \end{cases}$$

On a $\sigma_a(q) > q \Longleftrightarrow q \leq a$, donc l'application $a \longmapsto \sigma_a$ est injective de $\mathbb{R}$ dans $\mathfrak{S}_{\mathbb{Q}}$; comme $\mathbb{R}$ n'est pas dénombrable, $\mathfrak{S}_{\mathbb{Q}}$ ne l'est pas non plus.