Agrégation Externe

Un sujet type 0

Exercices

– I – Analyse réelle

1. Soient T_1, T_2 deux réels non nuls et f une fonction continue de $\mathbb{R}$ dans $\mathbb{R}$, telle que :

$$\forall x \in \mathbb{R},\ f(x+T_1) = f(x+T_2) = f(x)$$

Montrer que si $\dfrac{T_1}{T_2}$ est irrationnel, la fonction f est alors constante.

Solution : L'ensemble $\mathcal{P}(f)$ de toutes les périodes de f est un sous-groupe de $(\mathbb{R}, +)$.
On rappelle que le groupe additif engendré par T_1 et T_2 :

$$\mathbb{Z}T_1 + \mathbb{Z}T_2 = \left\{pT_1 + qT_2 \mid (p,q) \in \mathbb{Z}^2\right\}$$

est discret [resp. dense dans $\mathbb{R}$] si, et seulement si, $\dfrac{T_1}{T_2}$ est rationnel [resp. irrationnel].
Comme T_1 et T_2 sont dans le groupe $\mathcal{P}(f)$, on a $\mathbb{Z}T_1 + \mathbb{Z}T_2 \subset \mathcal{P}(f)$.
Si $\dfrac{T_1}{T_2}$ irrationnel, le groupe $\mathbb{Z}T_1 + \mathbb{Z}T_2$ est alors dense dans $\mathbb{R}$ et il en est de même de $\mathcal{P}(f)$ et comme ce groupe est fermé pour f continue, on a $\mathcal{P}(f) = \mathbb{R}$, ce qui revient à dire que f est constante.

2. Soient T_1, T_2 deux réels non nuls et f une fonction de $\mathbb{R}$ dans $\mathbb{R}$ admettant une limite à gauche [resp. à droite] en un point a et telle que :

$$\forall x \in \mathbb{R},\ f(x+T_1) = f(x+T_2) = f(x)$$

Montrer que si $\dfrac{T_1}{T_2}$ est irrationnel, la fonction f est alors constante.

3. **Solution :** Les réels T_1 et T_2 sont dans le groupe $\mathcal{P}(f)$, donc $\mathbb{Z}T_1 + \mathbb{Z}T_2 \subset \mathcal{P}(f)$.
Si $\dfrac{T_1}{T_2}$ irrationnel, le groupe $\mathbb{Z}T_1 + \mathbb{Z}T_2$ est alors dense dans $\mathbb{R}$ et il en est de même de $\mathcal{P}(f)$.
Pour tout réel x, on peut trouver une suite strictement croissante $(T_n)_{n\in\mathbb{N}}$ d'éléments de $\mathcal{P}(f)$ qui converge vers $a - x$, donc la suite $(x + T_n)_{n\in\mathbb{N}}$ converge en croissant vers a et on a :

$$\ell = \lim_{\substack{x\to a \\ x<a}} f(x) = \lim_{n\to+\infty} f(x+T_n) = f(x)$$

La fonction f est donc constante.

4. Montrer que pour tout entier naturel n et toutes suites de réels $(a_k)_{0\le k\le n}$ et $(\lambda_k)_{0\le k\le n}$, les a_k étant non tous nuls et les λ_k deux à deux distincts, la fonction f_n définie par :

$$f_n(x) = \sum_{k=0}^{n} a_k x^{\lambda_k}$$

a au plus n racines réelles distinctes dans $\mathbb{R}^{+,*}$.
Solution : On procède par récurrence sur $n \ge 0$.
Pour $n = 0$, $f_0(x) = a_0 x^{\lambda_0}$ n'a pas de racine dans $\mathbb{R}^{+,*}$ puisque a_0 est non nul.
Supposons le résultat acquis au rang $n \ge 0$. Si la fonction $f_{n+1} = \sum_{k=0}^{n+1} a_k x^{\lambda_k}$ a plus de $n+1$ racines distinctes dans $\mathbb{R}^{+,*}$, il en est alors de même de la fonction :

$$g_{n+1}(x) = x^{-\lambda_j} f_{n+1}(x) = \sum_{k=0}^{n+1} a_k x^{\lambda_k - \lambda_j}$$

où j compris entre 0 et $n+1$ est choisi tel que $a_j \neq 0$. Le théorème de Rolle nous dit alors que la fonction dérivée :

$$g'_{n+1}(x) = \sum_{k=0}^{n+1} (\lambda_k - \lambda_j) a_k x^{\lambda_k - \lambda_j - 1} = \sum_{\substack{k=0 \\ k \neq j}}^{n+1} (\lambda_k - \lambda_j) a_k x^{\lambda_k - \lambda_j - 1}$$

a plus de n racines distinctes dans $\mathbb{R}^{+,*}$ et en conséquence tous les $(\lambda_k - \lambda_j) a_k$ pour $k \neq j$ sont nuls (hypothèse de récurrence), ce qui entraîne $f_{n+1}(x) = a_j x^{\lambda_j}$, mais cette fonction ne s'annule jamais sur $\mathbb{R}^{+,*}$. On aboutit donc à une impossibilité.

– II – Suites et séries de fonctions

1. Montrer que la fonction $f : x \mapsto \sum_{n=0}^{+\infty} e^{-\left(n+in^2x\right)}$ est bien définie et indéfiniment dérivable sur $\mathbb{R}$, mais non développable en série entière en 0.
Solution : Notons $u_n(x) = e^{-\left(n+in^2x\right)}$.
Pour tout entier naturel n et tout réel x, on a $|u_n(x)| = e^{-n}$, donc la série de fonctions $\sum u_n$ converge normalement sur $\mathbb{R}$.
Toutes les fonctions u_n sont de classe $\mathcal{C}^\infty$ sur $\mathbb{R}$ avec, pour tout entier naturel p :

$$\left|u_n^{(p)}(x)\right| = n^{2p} e^{-n} = \underset{n\to+\infty}{o}\left(e^{-\frac{n}{2}}\right)$$

donc la série de fonctions $\sum u_n^{(p)}$ converge normalement sur $\mathbb{R}$.
Il en résulte que f est p fois dérivable sur $\mathbb{R}$ avec, pour tout réel x :

$$f^{(p)}(x) = (-i)^p \sum_{n=0}^{+\infty} n^{2p} e^{-\left(n+in^2x\right)}$$

Pour $x = 0$, on a :

$$\left|f^{(p)}(0)\right| = \sum_{n=0}^{+\infty} n^{2p} e^{-n}$$

et :

$$a_p = \frac{\left|f^{(p)}(0)\right|}{p!} \geq \frac{p^{2p} e^{-p}}{p!} \geq p^p e^{-p}$$

ce qui nous donne :

$$\sqrt[p]{a_p} \geq \frac{p}{e} \underset{p\to+\infty}{\to} +\infty$$

Le rayon de convergence de la série de Taylor $\sum \frac{f^{(p)}(0)}{p!} x^p$ est donc $R = 0$ et f ne peut être développable en série entière en 0.

2. Montrer que la fonction $f : x \mapsto \int_0^{+\infty} e^{-\sqrt{t}} e^{-ixt} dt$ est bien définie et indéfiniment dérivable sur $\mathbb{R}$, mais non développable en série entière en 0.
Solution : Pour tout réel x, la fonction $t \mapsto e^{-\sqrt{t}} e^{-ixt}$ est continue sur $\mathbb{R}^+$ et $\left|e^{-\sqrt{t}} e^{-ixt}\right| = e^{-\sqrt{t}} = \underset{t\to+\infty}{o}\left(\frac{1}{t^2}\right)$, donc cette fonction est intégrable sur $\mathbb{R}^+$.

Pour tout entier naturel n et tout réel positif t, la fonction $t \mapsto \dfrac{\partial^n}{\partial x^n}\left(e^{-\sqrt{t}}e^{-ixt}\right) = (-it)^n e^{-\sqrt{t}}e^{-ixt}$ est continue sur $\mathbb{R}^+$ avec :

$$\left|\frac{\partial^n}{\partial x^n}\left(e^{-\sqrt{t}}e^{-ixt}\right)\right| = t^n e^{-\sqrt{t}} = \underset{t\to+\infty}{o}\left(\frac{1}{t^2}\right)$$

On déduit alors du théorème de dérivation de Lebesgue que la fonction f est n fois dérivable avec, pour tout réel x :

$$f^{(n)}(x) = (-i)^n \int_0^{+\infty} t^n e^{-\sqrt{t}}e^{-ixt}dt$$

Pour $x = 0$, on a :

$$\left|f^{(n)}(0)\right| = \int_0^{+\infty} t^n e^{-\sqrt{t}}dt = 2\int_0^{+\infty} x^{2n+1}e^{-x}dx = 2(2n+1)!$$

et :

$$a_n = \frac{\left|f^{(n)}(0)\right|}{n!} = \frac{(2n+1)!}{n!}$$

ce qui nous donne :

$$\frac{a_{n+1}}{a_n} = \frac{(2n+3)(2n+2)}{n+1} \underset{p\to+\infty}{\to} +\infty$$

Le rayon de convergence de la série de Taylor $\sum \dfrac{f^{(n)}(0)}{n!}x^n$ est donc $R = 0$ et f ne peut être développable en série entière en 0.

– III – Longueur de courbes

Pour toute fonction $f : [a,b] \to \mathbb{R}$ de classe $\mathcal{C}^1$, on note :

$$L(f) = \int_a^b \sqrt{1 + (f'(t))^2}dt$$

la longueur de la courbe représentative de f.

Étant données deux fonctions de classe $\mathcal{C}^1$ sur $[a,b]$ telles que :

- $f(a) = g(a)$, $f(b) = g(b)$;
- $f(t) \leq g(t)$ pour tout $t \in [a,b]$;
- g est convexe.

On se propose de montrer que $L(f) \geq L(g)$, l'égalité étant réalisée si et seulement $f = g$.

On désigne par φ la fonction définie sur $\mathbb{R}$ par :

$$\forall t \in \mathbb{R},\ \varphi(t) = \sqrt{1+t^2}$$

1. Pour cette question, $a < b$ sont deux réels, $I = [a,b]$, f est une fonction à valeurs réelles positives de classe $\mathcal{C}^1$ et g est une fonction à valeurs réelles continue sur I.

   (a) Montrer que si f est décroissante sur I, il existe alors un réel $c \in I$ tel que :

   $$\int_a^b f(t)\,g(t)\,dt = f(a)\int_a^c g(t)\,dt$$

   Solution : Voir cours.

(b) Montrer que si g est monotone sur I, il existe alors un réel $c \in I$ tel que :

$$\int_a^b f(t)\, g(t)\, dt = f(a) \int_a^c g(t)\, dt + f(b) \int_c^b g(t)\, dt$$

(deuxième formule de la moyenne).
Solution : Voir cours.

2. Montrer que pour tous réels x et y, on a :

$$\varphi(y) \geq \varphi(x) + (y-x)\, \varphi'(x)$$

l'inégalité étant stricte pour $x \neq y$.
Solution : En utilisant la formule de Taylor à l'ordre 2, on a pour $x \neq y$:

$$\varphi(y) = \varphi(x) + (y-x)\, \varphi'(x) + \frac{(y-x)^2}{2} \varphi''(t_{x,y})$$

où $t_{x,y}$ est un réel strictement compris entre x et y. Comme :

$$\varphi''(t) = \frac{1}{(1+t^2)^{\frac{3}{2}}} > 0$$

pour tout réel t, on en déduit que :

$$\varphi(y) > \varphi(x) + (y-x)\, \varphi'(x)$$

3. En déduire que :

$$L(f) \geq L(g) + \int_a^b (f'(t) - g'(t))\, \varphi' \circ g'(t)\, dt$$

Solution : On a :

$$\int_a^b \varphi(f'(t))\, dt \geq \int_a^b \varphi(g'(t))\, dt + \int_a^b (f'(t) - g'(t))\, \varphi'(g'(t))\, dt$$

soit :

$$L(f) \geq L(g) + \int_a^b (f'(t) - g'(t))\, \varphi' \circ g'(t)\, dt$$

4. En supposant que g est de classe $\mathcal{C}^2$ sur $[a,b]$, montrer que :

$$\int_a^b (f'(t) - g'(t))\, \varphi' \circ g'(t)\, dt \geq 0$$

et conclure.
Solution : Une intégration par parties donne :

$$\begin{aligned}\int_a^b (f'(t) - g'(t))\, \varphi' \circ g'(t)\, dt &= \left[(f(t) - g(t))\, \varphi' \circ g'(t)\right]_a^b - \int_a^b (f(t) - g(t))\, (\varphi' \circ g')'(t)\, dt \\ &= -\int_a^b (f(t) - g(t))\, \varphi''(g'(t))\, g''(t)\, dt\end{aligned}$$

(on a $f(a) = g(a)$, $f(b) = g(b)$) avec $\varphi''(x) > 0$ pour tout réel x, $f(t) \leq g(t)$ et $g''(t) \geq 0$ pour tout $t \in [a,b]$ (g est convexe).
Il en résulte que $L(f) \geq L(g)$.

Pour $f \neq g$, on a $f' \neq g'$ ($f' = g'$ équivaut à $f = g$ puisque $f(a) = g(a)$), donc il existe $t_0 \in [a,b]$ tel que $f'(t_0) \neq g'(t_0)$ et, pour tout $t \in [a,b]$, on a :

$$\varphi(f'(t)) \geq \varphi(g'(t)) + (f'(t) - g'(t))\,\varphi'(g'(t))$$

l'inégalité étant stricte en t_0. Par continuité, on en déduit que :

$$L(f) > L(g) + \int_a^b (f'(t) - g'(t))\,\varphi' \circ g'(t)\,dt \geq L(g)$$

Donc l'égalité est réalisée si, et seulement si, $f = g$.

5. On suppose que g est seulement de classe $\mathcal{C}^1$ sur $[a,b]$. Montrer que l'inégalité $L(f) \geq L(g)$ est encore réalisée.
Solution : Comme la fonction $\varphi' \circ g'$ est continue, croissante à valeurs positive, la deuxième formule de la moyenne nous dit qu'il existe $c \in [a,b]$ tel que :

$$\begin{aligned}\int_a^b (f'(t) - g'(t))\,\varphi' \circ g'(t)\,dt &= \varphi'(g'(a)) \int_a^c (f'(t) - g'(t))\,dt + \varphi'(g'(b)) \int_c^b (f'(t) - g'(t))\,dt \\ &= \varphi'(g'(a))\,(f(c) - g(c)) - \varphi'(g'(b))\,(f(c) - g(c)) \\ &= (g(c) - f(c))\,(\varphi'(g'(b)) - \varphi'(g'(a))) \geq 0\end{aligned}$$

– IV – Algèbre générale

1. Montrer que l'anneau $\mathbb{D}$ des nombres décimaux est principal.
Solution : Si I est un idéal de $\mathbb{D}$ non réduit à $\{0\}$, $I \cap \mathbb{N}^*$ est alors non vide. En effet comme I est un sous-groupe additif de $\mathbb{D}$, il contient un décimal $d > 0$ (si $d \in I \setminus \{0\}$, alors $-d \in I \setminus \{0\}$) et en écrivant $d = \dfrac{a}{10^p}$ avec $a \in \mathbb{N}^*$ et $p \in \mathbb{N}$, on a $a = 10^p d \in I$ puisque I est un idéal de $\mathbb{D}$ et $10^p \in \mathbb{D}$.
En tant que partie non vide de $\mathbb{N}^*$, $I \cap \mathbb{N}^*$ admet donc un plus petit élément α.
Du fait que I est un idéal de $\mathbb{D}$ on déduit que $(\alpha) \subset I$.
D'autre part, tout $d \in I$ s'écrit $d = \dfrac{a}{10^p}$ avec $a \in \mathbb{Z}$ et $p \in \mathbb{N}$ et en effectuant la division euclidienne dans $\mathbb{Z}$ de $a = 10^p d$ par α, on a $10^p d = \alpha q + r$ avec $q \in \mathbb{Z}$ et $0 \leq r \leq \alpha - 1$ dans $\mathbb{N}$, ce qui donne $r = 10^p d - \alpha q \in I \cap \mathbb{N}$ ($10^p d$ et αq sont dans $\mathbb{D}$ puisque d et α y sont et I est un idéal) et nécessairement $r = 0$ par définition de α. On a $d = \alpha \dfrac{q}{10^p} \in \alpha\mathbb{D}$ et $I \subset (\alpha)$, soit en définitive $I = (\alpha)$.
2. $\mathbb{A}$ désigne un anneau commutatif, unitaire, intègre et $\mathbb{K}$ est le corps des fraction de $\mathbb{A}$.
On se donne une partie S de $\mathbb{A}^*$ qui contient 1 et qui est stable pour le produit, c'est-à-dire que pour tout (a,b) dans S^2, le produit ab est dans S.
   (a) Montrer que l'ensemble :
   $$S^{-1}\mathbb{A} = \left\{ \frac{a}{s} \mid a \in \mathbb{A} \text{ et } s \in S \right\}$$
   est un sous-anneau du corps $\mathbb{K}$ qui contient $\mathbb{A}$.
   Solution : Comme $1 \in S$, on a $a = \dfrac{a}{1} \in S^{-1}\mathbb{A}$ pour tout $a \in \mathbb{A}$.
   Pour $x = \dfrac{a}{s}$, $y = \dfrac{b}{t}$ dans $S^{-1}\mathbb{A}$ avec a, b dans $\mathbb{A}$ et s, t dans S, on a :
   $$x - y = \frac{at - bs}{st} S^{-1}\mathbb{A} \text{ et } xy = \frac{ab}{st}$$
   puisque S est stable pour le produit et contenue dans $\mathbb{A}$.
   Donc $S^{-1}\mathbb{A}$ est bien un sous-anneau de $\mathbb{K}$ qui contient $\mathbb{A}$.

(b) Montrer que si $\mathbb{A}$ est principal, il en est alors de même de $S^{-1}\mathbb{A}$.
Solution : Supposons que $\mathbb{A}$ soit principal et soit J un idéal de $S^{-1}\mathbb{A}$.
L'ensemble :

$$I = \left\{ a \in \mathbb{A} \mid \exists s \in S \text{ tel que } \frac{a}{s} \in J \right\}$$

est alors un idéal de $\mathbb{A}$ contenu dans J.
En effet, $0 \in I$, donc I est non vide et pour $a \in I$ et $s \in S$ tel que $\frac{a}{s} \in J$, on a $a = \frac{a}{s}s \in J$ puisque J est un idéal, donc $I \subset J$.
Pour a, b dans I et s, t dans S, tels que $\frac{a}{s}$ et $\frac{b}{s}$ soient dans J, on a $\frac{a}{st} = \frac{a}{s}\frac{1}{t} \in J$ et $\frac{b}{st} = \frac{b}{t}\frac{1}{s} \in J$ puisque J est un idéal, ce qui nous donne :

$$\frac{a-b}{st} = \frac{a}{st} - \frac{b}{st} \in J$$

donc $a - b \in I$ et I est un sous-groupe additif de $\mathbb{A}$.
Enfin, pour tout $c \in \mathbb{A}$, on a $\frac{ac}{s} = \frac{a}{s}c \in J$, donc $ac \in I$ et I est un idéal de $\mathbb{A}$.
Comme $\mathbb{A}$ est principal, il existe $a_0 \in \mathbb{A}$ tel que $I = (a_0)$ et $(S^{-1}\mathbb{A}) \cdot a_0 \subset J$ (puisque $a_0 \in I \subset J$ et J est un idéal).
Enfin, pour $x = \frac{a}{s}$ dans J avec $a \in \mathbb{A}$ et $s \in S$, on a $a \in I$, donc $a = qa_0$ avec $q \in \mathbb{A}$ et $x = \frac{q}{s}a_0 \in (S^{-1}\mathbb{A}) \cdot a_0$.
En conclusion, $J = (S^{-1}\mathbb{A}) \cdot a_0$ est principal.

(c) Montrer que si $\mathbb{A}$ est euclidien, il en est alors de même de $S^{-1}\mathbb{A}$.
Solution : Supposons que $\mathbb{A}$ soit euclidien de stathme $\varphi : \mathbb{A}^* \to \mathbb{N}$.
Tout $x \in (S^{-1}\mathbb{A})^*$ s'écrit $x = \frac{a}{s}$ avec $a \in \mathbb{A}^*$ et $s \in S \subset \mathbb{A}^*$, donc $a = sx \in \mathbb{A}^*$ et $\varphi(a) = \varphi(sx) \in \mathbb{N}$, ce qui permet de définir le stathme φ' sur $S^{-1}\mathbb{A}$ par :

$$\forall x \in \left(S^{-1}\mathbb{A}\right)^*,\ \varphi'(x) = \min\{\varphi(sx) \mid s \in S \text{ et } sx \in \mathbb{A}^*\}$$

On vérifie alors que $S^{-1}\mathbb{A}$ est euclidien pour ce stathme φ'.
Soient x, y dans $S^{-1}\mathbb{A}$ avec $y \neq 0$ et s, t dans S tels que $a = sx \in \mathbb{A}$ et $b = ty \in \mathbb{A}^*$ avec $\varphi(b) = \varphi'(y)$.
Dans $\mathbb{A}$ on a une division euclidienne $a = bq + r$ avec $r = 0$ ou $r \neq 0$ et $\varphi(r) < \varphi(b)$, ce qui nous donne :

$$x = \frac{a}{s} = \frac{bq}{s} + \frac{r}{s} = \frac{qt}{s}\frac{b}{t} + \frac{r}{s} = q'y + r'$$

avec $r' = \frac{r}{s} = 0$ si $r = 0$ ou $r' \neq 0$ si $r \neq 0$ et :

$$\varphi'(r') \leq \varphi(sr') = \varphi(r) < \varphi(b) = \varphi'(y)$$

(d) Montrer que l'anneau $\mathbb{D}$ des nombres décimaux est euclidien (donc principal).
Solution : Prenant $\mathbb{A} = \mathbb{Z}$ et $S = \{10^n \mid n \in \mathbb{N}\}$, on en déduit que l'anneau $\mathbb{D}$ des nombres décimaux est euclidien.

(e) Montrer que l'ensemble :

$$\mathbb{A} = \left\{ \frac{P(X)}{X^n} \mid P \in \mathbb{C}[X] \text{ et } n \in \mathbb{N} \right\}$$

est un anneau euclidien.
Solution : Prenant $\mathbb{A} = \mathbb{C}[X]$ et $S = \{X^n \mid n \in \mathbb{N}\}$, on en déduit que l'anneau :

$$\mathbb{A} = \left\{ \frac{P(X)}{X^n} \mid P \in \mathbb{C}[X] \text{ et } n \in \mathbb{N} \right\}$$

est euclidien.

3. Montrer que l'anneau quotient $\dfrac{\mathbb{C}[X,Y]}{(XY-1)}$ est euclidien.

Solution : L'application :

$$\begin{array}{rccc}\varphi: & \mathbb{C}[X,Y] & \to & \mathbb{C}(X) \\ & P(X,Y) & \mapsto & P\left(X,\dfrac{1}{X}\right)\end{array}$$

est un morphisme d'anneaux.
En écrivant tout polynôme $P \in \mathbb{C}[X,Y] = \mathbb{C}[X][Y]$ sous la forme :

$$P(X,Y) = \sum_{k=0}^{n} A_k(X) Y^k$$

où les A_k sont dans $\mathbb{C}[X]$, on a :

$$\varphi(P)(X) = \sum_{k=0}^{n} \frac{A_k(X)}{X^k} = \frac{A(X)}{X^n} \in \mathbb{C}(X)$$

où $A \in \mathbb{C}[X]$, donc :

$$\mathrm{Im}(\varphi) \subset S^{-1}\mathbb{C}[X] \text{ où } S = \{X^n \mid n \in \mathbb{N}\}$$

En écrivant toute fraction rationnelle $T \in S^{-1}\mathbb{C}[X]$ sous la forme :

$$T(X) = \sum_{k=0}^{n} \frac{a_k X^k}{X^n} \text{ où } a_k \in \mathbb{C} \text{ pour } 0 \leq k \leq n$$

on a $T = \varphi(P)$ où $P(X,Y) = \sum_{k=0}^{n} a_k X^k Y^n$, donc $\mathrm{Im}(\varphi) = S^{-1}\mathbb{C}[X]$.
On vérifie que le noyau de φ est l'idéal $(XY-1)$.
Dans $\mathbb{C}(X)[Y]$, on peut effectuer la division euclidienne de tout polynôme $P \in \mathbb{C}[X,Y]$ par $XY-1$, soit :

$$P(X,Y) = Q(X,Y)(XY-1) + R(X,Y)$$

où $Q(X,Y) \in \mathbb{C}(X)[Y]$ et R est de degré en Y strictement inférieur à 1, soit $R = R(X) \in \mathbb{C}(X)$.
Donc P est dans le noyau de φ si, et seulement si, $R = 0$, ce qui revient à dire que $P(X,Y) = Q(X,Y)(XY-1)$.
Il s'agit alors de vérifier que Q est en fait dans $\mathbb{C}[X][Y]$.
Pour $Q = 0$ c'est clair et pour $Q \neq 0$, on a :

$$P(X,Y) = \sum_{k=0}^{n} A_k(X) Y^k \text{ et } Q(X,Y) = \sum_{k=0}^{n-1} B_k(X) Y^k$$

où les A_k sont dans $\mathbb{C}[X]$ et les B_k dans $\mathbb{C}(X)$.
L'égalité $P(X,Y) = Q(X,Y)(Y - X^2)$ nous donne alors :

$$\begin{aligned} P(X,Y) &= \sum_{k=0}^{n-1} XB_k(X) Y^{k+1} - \sum_{k=0}^{n-1} B_k(X) Y^k \\ &= \sum_{k=1}^{n} XB_{k-1}(X) Y^k - \sum_{k=0}^{n-1} B_k(X) Y^k \\ &= XB_{n-1}(X) Y^k - B_0(X) + \sum_{k=1}^{n-1} (XB_{k-1}(X) - B_k(X)) Y^k \end{aligned}$$

et, par récurrence finie, on en déduit que :

$$\begin{cases} B_0(X) = -A_0(X) \in \mathbb{C}[X] \\ B_k(X) = A_k(X) - XB_{k-1}(X) \in \mathbb{C}[X] \quad (1 \leq k \leq n-1) \end{cases}$$

soit $Q \in \mathbb{C}[X][Y]$.
En conclusion $\dfrac{\mathbb{C}[X,Y]}{(XY-1)} = \dfrac{\mathbb{C}[X,Y]}{\ker(\varphi)}$ est isomorphe à $S^{-1}\mathbb{C}[X]$ qui est euclidien, donc $\dfrac{\mathbb{C}[X,Y]}{(XY-1)}$ est euclidien et aussi principal et factoriel.

– IV – Algèbre linéaire (d'après agrégation 2008)

Si n est un entier naturel non nul et $\mathbb{K}$ un corps, on note $\mathcal{MT}(n,\mathbb{K})$ l'affirmation suivante :
Pour toutes matrices A et B diagonalisables dans $\mathcal{M}_n(\mathbb{K})$, la propriété :
(a) A et B commutent ;
est équivalente à la propriété :
(b) pour tout $\lambda \in \mathbb{K}$, $A + \lambda B$ est diagonalisable dans $\mathcal{M}_n(\mathbb{K})$.
On peut montrer que $\mathcal{MT}(n,\mathbb{C})$ est vraie pour tout $n \geq 1$ (théorème de Motzkin-Taussky, 1952).
On se propose de montrer ici que l'implication $(a) \Rightarrow (b)$ est vraie dans l'affirmation $\mathcal{MT}(n,\mathbb{K})$, pour tout entier $n \geq 1$ et tout corps $\mathbb{K}$, puis d'étudier l'implication $(b) \Rightarrow (a)$ dans les affirmations $\mathcal{MT}(2,\mathbb{R})$ et $\mathcal{MT}(2,\mathbb{C})$.

1. Soient $\mathbb{K}$ un corps et E un $\mathbb{K}$-espace vectoriel de dimension finie.
   On considère u et v deux endomorphismes diagonalisables de E qui commutent, c'est-à-dire tels que $u \circ v = v \circ u$.

   (a) Montrer que les sous-espaces propres de v sont stables par u, c'est-à-dire que si F est un sous-espace propre de v, on a $u(F) \subset F$.
   Solution :

   (b) Montrer que u induit sur chaque sous-espace propre de v un endomorphisme diagonalisable.
   Solution :

   (c) En déduire l'existence d'une base commune de réduction dans E pour les endomorphismes u et v, c'est-à-dire qu'il existe une base $\mathcal{B}$ de E telle que celle ci soit une base de vecteurs propres à la fois de u et de v.
   Solution :

2. Plus généralement, on considère $(u_i)_{i\in I}$ une famille d'endomorphismes diagonalisables de E. On suppose en outre que ces endomorphismes commutent deux à deux :

   $$\left(\forall (i,j) \in I^2\right),\ u_i \circ u_j = u_j \circ u_i$$

   Montrer l'existence d'une base commune de réduction dans E pour la famille $(u_i)_{i\in I}$, c'est-à-dire qu'il existe une base $\mathcal{B}$ de E qui est une base de vecteurs propres pour chaque endomorphisme u_i, $i \in I$.
   Solution :

3. Montrer que l'implication $(a) \Rightarrow (b)$ est vraie dans l'affirmation $\mathcal{MT}(n,\mathbb{K})$, pour tout entier $n \geq 1$ et tout corps $\mathbb{K}$.
   Solution :

4. Étudier l'implication $(b) \Rightarrow (a)$ dans l'affirmation $\mathcal{MT}(2,\mathbb{R})$.
   Solution :

5. On étudie l'implication $(b) \Rightarrow (a)$ dans l'affirmation $\mathcal{MT}(2, \mathbb{C})$.
Soit A et B deux matrices diagonalisables de $\mathcal{M}_2(\mathbb{C})$ satisfaisant à la propriété (b) de $\mathcal{MT}(2, \mathbb{C})$.

   (a) Montrer que l'on peut se ramener au cas où B est une matrice diagonale de $\mathcal{M}_2(\mathbb{C})$ avec au moins une valeur propre nulle.
   Solution :

   (b) En supposant que B est une matrice diagonale non nulle avec une valeur propre nulle, démontrer l'existence d'un nombre complexe λ_0 tel que $A + \lambda_0 B$ ait une valeur propre double.
   Solution :

   (c) En déduire que l'implication $(b) \Rightarrow (a)$ dans $\mathcal{MT}(2, \mathbb{C})$ est vraie.
   Solution :

Problème

Corps ordonnés

Ce problème a pour objet l'étude des corps commutatifs ordonnés, c'est-à-dire les corps munis d'une relation d'ordre total qui est compatible avec l'addition et la multiplication par les éléments positifs. Par exemple $\mathbb{Q}, \mathbb{R}$ ou tout corps compris entre les deux (les nombres algébriques ou les nombres constructibles).

Certaines questions peuvent sembler élémentaires. Il ne suffit pas d'affirmer que le résultat est évident, il faut donner une réponse concise mais rigoureuse en mettant bien en évidence les points qui permettent d'aboutir.

Les trois parties de ce problème sont indépendantes.

– I – Corps ordonnables

Soit $\mathbb{K}$ un corps commutatif.

On note $+$ l'addition sur $\mathbb{K}$ et $\cdot$ la multiplication (on écrira aussi xy pour $x \cdot y$).

Pour toutes parties A, B de $\mathbb{K}$, on note :

$$\begin{cases} -A = \{-x \mid x \in A\} \\ A^2 = \{x^2 \mid x \in A\} \\ A + B = \{x + y \mid (x, y) \in A \times B\} \\ A \cdot B = \{x \cdot y \mid (x, y) \in A \times B\} \end{cases}$$

On dit que $\mathbb{K}$ est ordonnable s'il existe une relation d'ordre total qui est compatible avec la structure de corps de $\mathbb{K}$, c'est-à-dire une relation noté $\leq$ telle que :

– $\leq$ est une relation d'ordre total sur $\mathbb{K}$;

– pour tous x, y, z dans $\mathbb{K}$ on a :

$$\begin{cases} x \leq y \Rightarrow x + z \leq y + z \\ x \leq y \text{ et } 0 \leq z \Rightarrow x \cdot z \leq y \cdot z \end{cases}$$

Si $\mathbb{K}$ est ordonnable, on dira alors que $(\mathbb{K}, \leq)$ est un corps ordonné.

Si $x \leq y$ dans $\mathbb{K}$, on pourra écrire de manière équivalente $y \geq x$.

On note :

$$\mathbb{K}^+ = \{x \in \mathbb{K} \mid 0 \leq x\}$$

Le corps des réels est muni de sa structure ordonnée usuelle et ses propriétés classiques (propriété d'Archimède, existence des bornes supérieures, ...) sont connues.

1. Soit $(\mathbb{K}, \leq)$ un corps ordonné. Montrer que pour toute suite finie $(x_i)_{1 \leq i \leq n}$ d'éléments de $\mathbb{K}$ on a $0 \leq \sum_{i=1}^{n} x_i^2$, l'égalité étant réalisée si, et seulement si, tous les x_i sont nuls.

   Solution : On procède par récurrence sur $n \geq 1$.

   Pour $n = 1$, il s'agit de montrer que $0 \leq x^2$ pour tout x dans $\mathbb{K}$.

   Soit $x \in \mathbb{K}$. Si $0 \leq x$, on a alors $0 = 0 \cdot x \leq x^2$ et si $x \leq 0$ (l'ordre est total) alors $0 = x + (-x) \leq -x$ et $0 = 0 \cdot (-x) \leq (-x)^2 = x^2$. On a donc bien $0 \leq x^2$ dans tous les cas.

   Supposons le résultat acquis au rang $n \geq 1$ et soit $(x_i)_{1 \leq i \leq n+1}$ une suite d'éléments de $\mathbb{K}$. En ajoutant x_{n+1}^2 aux deux membres de l'inégalité $0 \leq \sum_{i=1}^{n} x_i^2$, on obtient $0 \leq x_{n+1}^2 \leq \sum_{i=1}^{n+1} x_i^2$ et

$0 \leq \sum_{i=1}^{n+1} x_i^2$ par transitivité.

Si $\sum_{i=1}^{n} x_i^2 = 0$, pour tout j compris entre 1 et n, on a :

$$0 \leq x_j^2 \leq \sum_{i=1}^{n} x_i^2 = 0$$

$x_j^2 = 0$ (la relation $\leq$ est antisymétrique), ce qui équivaut à $x_j = 0$ (on est dans un corps).
En prenant tous les x_i égaux à 1, on a $0 \leq n \cdot 1$ pour tout entier naturel n, ce qui peut se traduire par $\mathbb{N} \subset \mathbb{K}^+$.

2. Montrer qu'un corps ordonnable est nécessairement de caractéristique nulle.
Solution : Soit $\mathbb{K}$ un corps de caractéristique p (entier naturel premier). Si $\mathbb{K}$ est ordonné, on a $0 \leq 1 \leq p \cdot 1 = 0$ et $1 = 0$, ce qui est impossible dans un corps.

3. Montrer qu'un corps algébriquement clos n'est pas ordonnable.
Solution : Soit $\mathbb{K}$ un corps algébriquement clos et i une racine de $X^2 + 1 = 0$. Supposons que $\mathbb{K}$ soit ordonné. Si $0 \leq i$ [resp. $i \leq 0$], on a alors $0 = 0 \cdot i \leq i^2 = -1$ [resp. $0 = (-i) + i \leq -i$, ce qui donne $0 = 0 \cdot (-i) \leq (-i)^2 = -1$] et $1 = 1 + 0 \leq 1 + (-1) = 0$, ce qui est impossible. Donc $\mathbb{K}$ n'est pas ordonnable. C'est le cas par exemple pour le corps $\mathbb{C}$ des nombres complexes.

4. Soit $(\mathbb{K}, \leq)$ un corps ordonné. Pour tout polynôme P dans $\mathbb{K}[X]$, on note :

$$d(P) = \begin{cases} 0 \text{ si } P = 0 \\ a_n \text{ si } P(X) = \sum_{k=0}^{n} a_k X^k \text{ est de degré } n. \end{cases}$$

On écrit toute fraction rationnelle R dans $\mathbb{K}(X)$ sous la forme $R = \dfrac{P}{Q}$ avec P, Q dans $\mathbb{K}[X]$ et Q non nul unitaire. On définit la relation $\leq$ sur $\mathbb{K}(X)$ par :

$$\frac{P_1}{Q_1} \leq \frac{P_2}{Q_2} \Leftrightarrow d(Q_1P_2 - P_1Q_2) \geq 0.$$

Montrer que cette relation est bien définie et que $(\mathbb{K}(X), \leq)$ un corps ordonné.
Solution : Il s'agit d'abord de montrer que la définition de $\leq$ ne dépend pas des choix des numérateurs et dénominateurs des fractions rationnelles. Soient $R_1 = \dfrac{P_1}{Q_1} = \dfrac{U_1}{V_1}$ et $R_2 = \dfrac{P_2}{Q_2} = \dfrac{U_2}{V_2}$ dans $\mathbb{K}(X)$. Supposons que $d(Q_1P_2 - P_1Q_2) \geq 0$. Les polynômes V_1 et V_2 étant unitaires, on a :

$$d(V_1V_2(Q_1P_2 - P_1Q_2)) = d(Q_1P_2 - P_1Q_2) \geq 0$$

et tenant compte de $P_1V_1 = U_1Q_1$, $P_2V_2 = U_2Q_2$, on déduit que :

$$d(V_1U_2 - V_2U_1) = d(Q_1Q_2(V_1U_2 - V_2U_1)) \geq 0,$$

(Q_1Q_2 est unitaire). La relation $\leq$ est donc bien définie.
Cette relation est d'ordre. En effet :
– $\dfrac{P}{Q} \leq \dfrac{P}{Q}$ puisque $d(0) = 0$;
– si $\dfrac{P_1}{Q_1} \leq \dfrac{P_2}{Q_2}$ et $\dfrac{P_2}{Q_2} \leq \dfrac{P_1}{Q_1}$ alors $0 \leq d(Q_1P_2 - P_1Q_2) \leq 0$ et $Q_1P_2 - P_1Q_2 = 0$, soit $\dfrac{P_1}{Q_1} = \dfrac{P_2}{Q_2}$;
– si $\dfrac{P_1}{Q_1} \leq \dfrac{P_2}{Q_2}$ et $\dfrac{P_2}{Q_2} \leq \dfrac{P_3}{Q_3}$ alors

$$\begin{cases} d(Q_3(Q_1P_2 - P_1Q_2)) = d(Q_1P_2 - P_1Q_2) \geq 0 \\ d(Q_1(Q_2P_3 - P_2Q_3)) = d(Q_2P_3 - P_2Q_3) \geq 0 \end{cases}$$

(Q_1 et Q_2 sont unitaires) et en ajoutant on obtient

$$d(Q_1P_3 - P_1Q_3) = d(Q_2(Q_1P_3 - P_1Q_3)) \geq 0$$

(la somme de deux polynômes de coefficient dominant positif est un polynôme de même nature), ce qui équivaut à $\dfrac{P_1}{Q_1} \leq \dfrac{P_3}{Q_3}$.

L'ordre est total puisqu'il est total sur $\mathbb{K}$.

Si $\dfrac{P_1}{Q_1} \leq \dfrac{P_2}{Q_2}$ et $\dfrac{P_3}{Q_3} \in \mathbb{K}(X)$, alors :

$$\frac{P_j}{Q_j} + \frac{P_3}{Q_3} = \frac{P_jQ_3 + P_3Q_j}{Q_jQ_3} \quad (j = 1, 2)$$

et :

$$\begin{aligned} &d(Q_1Q_3(P_2Q_3 + P_3Q_2) - Q_2Q_3(P_1Q_3 + P_3Q_1)) \\ &= d(Q_1(P_2Q_3 + P_3Q_2) - Q_2(P_1Q_3 + P_3Q_1)) \\ &= d(Q_1P_2Q_3 - Q_2P_1Q_3) = d(Q_1P_2 - Q_2P_1) \geq 0 \end{aligned}$$

De même pour $\dfrac{P_3}{Q_3} \geq 0$, on a $\dfrac{P_j}{Q_j}\dfrac{P_3}{Q_3} = \dfrac{P_jP_3}{Q_jQ_3}$ pour $j = 1, 2$ et :

$$d(P_2P_3Q_1Q_3 - P_1P_3Q_2Q_3) = d(P_3)\,d(P_2Q_1 - P_1Q_2) \geq 0$$

puisque $d(P_3) \geq 0$.

L'ordre est donc bien compatible avec la structure de corps de $\mathbb{K}(X)$.

5. Montrer qu'un corps commutatif $\mathbb{K}$ est ordonnable si, et seulement si, il existe une partie P de $\mathbb{K}$ telle que :

$$\begin{cases} P \cap (-P) = \{0\} \\ P \cup (-P) = \mathbb{K} \\ P + P \subset P \\ P \cdot P \subset P \end{cases} \tag{1}$$

Solution : Soit $(\mathbb{K}, \leq)$ un corps ordonné. Montrons que l'ensemble $P = \mathbb{K}^+$ vérifie les propriétés annoncées.

- Si $x \in P \cap (-P)$, on a $0 \leq x$ et $x = -y$ avec $0 \leq y$. De $x \leq x$ (réflexivité de $\leq$) et $0 \leq -x$, on déduit que $x = x + 0 \leq 0 = x + (-x)$. On a donc $0 \leq x$ et $x \leq 0$, ce qui équivaut à $x = 0$ (antisymétrie de $\leq$).
- Soit x dans $\mathbb{K}$. On a soit $x \in P$, soit $x \notin P$ et dans ce cas $x \leq 0$ (l'ordre est total). En ajoutant $-x$ aux deux membres de cette inégalité on obtient $0 \leq y = -x$ et $x = -y$ est dans $-P$. On a donc bien $P \cup (-P) = \mathbb{K}$.
- Si x, y sont dans P, on a $0 \leq x$, $0 \leq y$, donc $x \leq x + y$ et $0 \leq x + y$ par transitivité. On a donc bien $P + P \subset P$.
- De même $0 \leq x$ et $0 \leq y$ donne $0 \leq xy$ et on a bien $P \cdot P \subset P$.

Réciproquement supposons qu'il existe une partie P de $\mathbb{K}$ vérifiant les propriétés (1). On définit la relation $\leq$ sur $\mathbb{K}$ par :

$$x \leq y \Leftrightarrow y - x \in P.$$

Vérifions que $\leq$ est une relation d'ordre total compatible avec la structure de corps de $\mathbb{K}$.

- Pour tout x dans $\mathbb{K}$ on a $x - x = 0 \in P$, donc $x \leq x$. La relation est réflexive.
- Si x, y dans $\mathbb{K}$ sont tels que $x \leq y$ et $y \leq x$, on a $y - x \in P$ et $x - y \in P$, donc $y - x = -(x - y) \in P \cap (-P)$ et $y = x$. La relation est antisymétrique.

– Si x, y, z dans $\mathbb{K}$ sont tels que $x \leq y$ et $y \leq z$, on déduit que $z - x = (y - x) + (z - y)$ est aussi dans P, c'est-à-dire que $x \leq z$. La relation est antisymétrique.
– Avec $P \cup (-P) = \mathbb{K}$ on déduit que l'ordre est total.
– Si $x \leq y$ dans $\mathbb{K}$, pour tout z dans $\mathbb{K}$ on a $(y + z) - (x + z) \in P$, donc $x + z \leq y + z$.
– Si $x \leq y$ et $0 \leq z$ dans $\mathbb{K}$, avec $P \cdot P \subset P$ on déduit que $z(y - x) \in P$ et $xz \leq yz$.

L'équivalence est donc démontrée.

6. Montrer que si $(\mathbb{L}, \leq)$ est un corps ordonné, alors tout sous-corps de $\mathbb{L}$ est naturellement ordonnable par $\leq$.
Solution : Si $\mathbb{K}$ est un sous corps de $\mathbb{L}$ alors le sous-ensemble $P = \mathbb{K} \cap \mathbb{L}^+$ de $\mathbb{K}$ vérifie les propriétés (1) , il en résulte que $\mathbb{K}$ est ordonnable par $\leq$.

7. Montrer que si $(\mathbb{L}, \leq)$ est un corps ordonné, alors tout corps isomorphe à $\mathbb{L}$ est naturellement ordonnable.
Solution : Soit σ un isomorphisme de $\mathbb{L}$ sur un corps commutatif $\mathbb{K}$. On montre facilement que le sous-ensemble $P = \sigma(\mathbb{L}^+)$ de $\mathbb{K}$ vérifie les propriétés (1) , ce qui implique que $\mathbb{K}$ est ordonnable par :
$$x \leq' y \Leftrightarrow y - x \in \sigma\left(\mathbb{L}^+\right).$$
En écrivant que $x = \sigma(u)$, $y = \sigma(v)$ avec u, v uniquement déterminés dans $\mathbb{K}$, la condition $y - x = \sigma(w)$ avec w dans $\mathbb{L}^+$ équivaut à $v - u = w \in \mathbb{L}^+$, soit à $u \leq v$. La relation d'ordre sur $\mathbb{K}$ est donc naturellement définie par :
$$x \leq' y \text{ dans } \mathbb{K} \Leftrightarrow \sigma^{-1}(x) \leq \sigma^{-1}(y) \text{ dans } \mathbb{L}.$$

8. Montrer qu'il existe une unique relation d'ordre total sur $\mathbb{Q}$ qui est compatible avec la structure de corps.
Solution : $\mathbb{Q}$ est déjà ordonné avec l'ordre usuel.
Soit $\leq$ une relation d'ordre total sur $\mathbb{Q}$ compatible avec la structure de corps. On a $1 \in \mathbb{Q}^+$ et par récurrence on vérifie facilement que pour tout entier naturel n on a $n \cdot 1 \in \mathbb{Q}^+$, c'est-à-dire que $\mathbb{N} \subset \mathbb{Q}^+$, ce qui implique que pour tout $n \in \mathbb{N}^*$, $\frac{1}{n} \cdot 1$ est dans $\mathbb{Q}^+$ (en effet, $\frac{1}{n} \cdot 1 \in (-\mathbb{Q}^+)$ entraîne $1 = n\frac{1}{n}1 \in (-\mathbb{Q}^+)$ et $1 = 0$, ce qui est faux). Avec $\mathbb{Q}^+ \cdot \mathbb{Q}^+ \subset \mathbb{Q}^+$, on déduit que :
$$P = \left\{ \frac{p}{q} \mid p \in \mathbb{N}, q \in \mathbb{N}^*, p \wedge q = 1 \right\} \subset \mathbb{Q}^+.$$
Réciproquement si $r = \frac{p}{q}$ est dans $\mathbb{Q}^+$ avec $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$, $p \wedge q = 1$, on a $p = qr \in \mathbb{Z} \cap \mathbb{Q}^+ = \mathbb{N}$ (en effet si p est négatif, alors $-p \in \mathbb{N} \subset \mathbb{Q}^+$ et $-r = \frac{1}{q}(-p) \in \mathbb{Q}^+$, ce qui impose $r = 0$). On a donc $P = \mathbb{Q}^+$, ce qui détermine de manière unique l'ordre compatible sur $\mathbb{Q}$.

9. Montrer qu'il existe une unique relation d'ordre total sur $\mathbb{R}$ qui est compatible avec la structure de corps.
Solution : $\mathbb{R}$ est déjà ordonné avec l'ordre usuel.
Soit $\leq$ une relation d'ordre total sur $\mathbb{R}$ compatible avec la structure de corps. On a vu que $\mathbb{R}^2 \subset \mathbb{R}^+$ (question **I.1**). D'autre part, avec $\mathbb{R} = \mathbb{R}^2 \cup (-\mathbb{R}^2)$ (si x est positif au sens usuel alors $x = \sqrt{x}^2$, sinon $x = -\sqrt{-x}^2$) et $\mathbb{R} = \mathbb{R}^+ \cup (-\mathbb{R}^+)$, on déduit que $\mathbb{R}^+ \subset \mathbb{R}^2$ (en effet si $x = -y^2$ est dans $\mathbb{R}^+$ et dans $-\mathbb{R}^2$ alors $-x$ est dans $\mathbb{R}^2 \subset \mathbb{R}^+$ et x qui est dans $\mathbb{R}^+ \cap (-\mathbb{R}^+)$ est nul). On a donc $\mathbb{R}^+ = \mathbb{R}^2$, ce qui détermine de manière unique l'ordre compatible sur $\mathbb{R}$.

10. Soit $\mathbb{K}$ un corps de caractéristique différente de 2. On note $\sum \mathbb{K}^2$ le sous-ensemble de $\mathbb{K}$ dont les éléments peuvent s'écrire comme somme finie de carrés. Montrer que les propriétés suivantes sont équivalentes :

(a) $\mathbb{K}$ est ordonnable ;

(b) $\mathbb{K} \neq \sum \mathbb{K}^2$;

(c) -1 n'est pas somme de carrés dans $\mathbb{K}$;

(d) une somme de carrés $\sum_{i=1}^{n} x_i^2$ est nulle dans $\mathbb{K}$ si, et seulement si, tous les x_i sont nuls ;

(e) il existe une partie non vide P de $\mathbb{K}$ telle que $\mathbb{K}^2 \subset P$, $P + P \subset P$, $P \cdot P \subset P$ et $P \cap (-P) = \{0\}$.

Solution : $(i) \Rightarrow (ii)$ On suppose que $(\mathbb{K}, \leq)$ est ordonné. Avec $\mathbb{K}^2 \subset \mathbb{K}^+$ (question **I.1**) et $\mathbb{K}^+ + \mathbb{K}^+ \subset \mathbb{K}^+$ on déduit que $\sum \mathbb{K}^2 \subset \mathbb{K}^+$ et comme $\mathbb{K}^+ \subsetneq \mathbb{K}$ (-1 qui est non nul et dans $-\mathbb{K}^+$ n'est pas dans $\mathbb{K}^+$), on déduit que $\sum \mathbb{K}^2 \subsetneq \mathbb{K}$.

$(ii) \Rightarrow (iii)$ Supposons que $\sum \mathbb{K}^2 \subsetneq \mathbb{K}$. Si $-1 \in \sum \mathbb{K}^2$, pour tout x dans $\mathbb{K}$ on a $(-1)\left(1 - \dfrac{x+1}{2}\right)^2 \in \sum \mathbb{K}^2$ (comme $\mathbb{K}$ est de caractéristique différente de 2, on peut diviser par 2 dans ce corps) et donc $x = -\left(1 - \dfrac{x+1}{2}\right)^2 + \left(\dfrac{x+1}{2}\right)^2$ est dans $\sum \mathbb{K}^2$, ce qui contredit l'hypothèse de départ.

$(iii) \Rightarrow (iv)$ Supposons que $-1 \notin \sum \mathbb{K}^2$ et soit $(x_i)_{1 \leq i \leq n}$ une suite d'éléments de $\mathbb{K}$ telle que $\sum_{i=1}^{n} x_i^2 = 0$. Si j est un indice tel que $x_j \neq 0$, on peut alors écrire que $-1 = \sum_{\substack{i=1 \\ i \neq j}}^{n} \left(\dfrac{x_i}{x_j}\right)^2$ est dans $\sum \mathbb{K}^2$ (si $n = 1$, le résultat est trivial), ce qui contredit l'hypothèse de départ.

$(iv) \Rightarrow (v)$ On suppose que 0 n'est pas somme de carrés non tous nuls. On pose $P = \sum \mathbb{K}^2$. On a facilement $\mathbb{K}^2 \subset P$, $P + P \subset P$ et $P \cdot P \subset P$. Si x est dans $P \cap (-P)$, il s'écrit $x = \sum_{i=1}^{n} x_i^2 = -\sum_{j=1}^{m} y_j^2$ et on a $\sum_{i=1}^{n} x_i^2 + \sum_{j=1}^{m} y_j^2 = 0$, ce qui entraîne que tous les x_i et tous les y_j sont nuls.

$(v) \Rightarrow (i)$ Soit :

$$E = \left\{ Q \subset \mathbb{K} \mid \mathbb{K}^2 \subset Q, Q + Q \subset Q, Q \cdot Q \subset Q, Q \cap (-Q) = \{0\} \right\}$$

– L'hypothèse (v) nous dit que E est non vide.
– Il est partiellement ordonné par $\subset$.
– Il est inductif (voir le rappel ci-après). En effet si A est une partie non vide totalement ordonnée de E, on montre alors que $M = \bigcup_{Q \in A} Q$ est dans E et majore A. $\mathbb{K}^2$ qui est contenu dans tous les $Q \in A$ est aussi contenu dans M. Si x, y sont dans M on a $x \in Q$ et $y \in Q'$ avec $Q \subset Q'$ ou $Q' \subset Q$ (A est totalement ordonné), donc $x + y$ est dans $Q' + Q' \subset Q'$ ou dans $Q + Q \subset Q$, il est donc dans M. On voit de même que $M \cdot M \subset M$. Enfin si $x \in M \cap (-M)$, on a $x \in Q$ et $-x \in Q'$, donc x est dans $Q \cap (-Q)$ ou dans $Q' \cap (-Q')$ et il est nul.

Le lemme de Zorn nous dit alors qu'il admet un élément maximal P.
Si on montre que $P \cup (-P) = \mathbb{K}$ on aura montré que $\mathbb{K}$ est ordonnable (question **I.5**).
Soit donc x dans $\mathbb{K}$ et supposons que x n'est pas dans P. Montrons que :

$$Q = P - xP = \left\{ y - xz \mid (y, z) \in P^2 \right\}$$

est dans E.

– On a $\mathbb{K}^2 \subset P \subset Q$, donc $\mathbb{K}^2 \subset Q$.
– Avec $P + P \subset P$, on déduit que $Q + Q \subset Q$.
– Si $u_1 = y_1 - xz_1$ et $u_2 = y_2 - xz_2$ sont dans Q, on a $u_1 u_2 = y_3 - xz_3$ avec $y_3 = y_1 y_2 + z_1 z_2 x^2$ dans $P \cdot P + P \cdot P \cdot \mathbb{K}^2 \subset P$ et $z_3 = z_1 y_2 + y_1 z_2$ dans $P \cdot P + P \cdot P \subset P$ puisque $\mathbb{K}^2 \subset P$, $P \cdot P \subset P$ et $P + P \subset P$. On a donc $Q \cdot Q \subset Q$.

– Si $u \in Q \cap (-Q)$, on a $u = y_1 - xz_1 = -(y_2 - xz_2)$ et $y_1 + y_2 = x(z_1 + z_2)$. Si $z_1 + z_2 = 0$, alors $y_1 + y_2 = 0$, ce qui implique que $y_1 = -y_2$ et $z_1 = -z_2$ sont dans $P \cap (-P) = \{0\}$ et $u = 0$. Si $z_1 + z_2 \neq 0$, alors $x = \left(\dfrac{1}{z_1 + z_2}\right)^2 (y_1 + y_2)(z_1 + z_2)$ est dans $\mathbb{K}^2 \cdot P \cdot P \subset P$, ce qui contredit $x \in P$. On a donc $Q \cap (-Q) = \{0\}$.

On a donc $Q \in E$ avec $P \subset Q$ et P maximal, ce qui implique $Q = P$ et $-x \in Q \subset P$, soit $x \in -P$.

L'équivalence des points (i) à (v) est donc montrée.

11. Montrer qu'un corps commutatif $\mathbb{K}$ est ordonnable si, et seulement si, -1 n'est pas somme de carrés dans $\mathbb{K}$ (théorème d'Artin-Schreier).
Solution : Si $\mathbb{K}$ est ordonnable, il est alors de caractéristique nulle et le point (iii) de la question précédente est vérifiée.
Réciproquement si (iii) est vérifié, alors $\mathbb{K}$ est de caractéristique différente de 2 ($-1 = 1^2$ dans un corps de caractéristique 2) et la question précédente nous dit que $\mathbb{K}$ est ordonnable.

Rappels sur le lemme (ou l'axiome) de Zorn

Soit $(E, \leq)$ un ensemble partiellement ordonné.

Soit A une partie de E. On dit que $m \in E$ est un majorant de A si $x \leq m$ pour tout x dans A.

On dit que $(E, \leq)$ est inductif si toute partie non vide et totalement ordonnée de E admet un majorant.

On dit qu'un élément m de E est maximal si, pour tout x dans E, la condition $m \leq x$ entraîne $x = m$.

Le lemme de Zorn affirme que : tout ensemble non vide ordonné et inductif admet un élément maximal.

Ce lemme (qui peut être pris comme un axiome) est équivalent à l'axiome du choix ou à l'axiome de Zermelo.

– II – Nombres algébriques et nombres transcendants

On dit qu'un nombre complexe α est algébrique s'il existe un polynôme non nul P dans $\mathbb{Q}[X]$ tel que $P(\alpha) = 0$.

Un nombre complexe qui n'est pas algébrique est dit transcendant.

On note $\mathbb{A}$ l'ensemble des nombres complexes algébriques.

Si A est un anneau commutatif unitaire et n un entier naturel non nul, on note $A[X_1, \cdots, X_n]$ l'anneau des polynômes à n indéterminées à coefficients dans A.

On dit qu'un polynôme P dans $A[X_1, \cdots, X_n]$ est symétrique s'il pour toute permutation σ de $\{1, 2, \cdots, n\}$ on a $P\left(X_{\sigma(1)}, \cdots, X_{\sigma(n)}\right) = P(X_1, \cdots, X_n)$.

Les polynômes symétriques élémentaires $(\sigma_k)_{1 \leq k \leq n}$ sont définis par :

$$\forall k \in \{1, 2, \cdots, n\}, \quad \sigma_k(X_1, \cdots, X_n) = \sum_{1 \leq i_1 < \cdots < i_k \leq n} X_{i_1} X_{i_2} \cdots X_{i_k}.$$

On rappelle que si $P \in A[X_1, \cdots, X_n]$ est symétrique, il existe alors un polynôme Q dans $A[X_1, \cdots, X_n]$ tel que $P(X_1, \cdots, X_n) = Q(\sigma_1, \cdots, \sigma_n)$.

1. Soit P un polynôme non constant et irréductible dans $\mathbb{Q}[X]$. Montrer que toutes les racines complexes de P sont simples.
Solution : Le polynôme P étant irréductible dans $\mathbb{Q}[X]$ est premier avec son polynôme dérivé P'. Le théorème de Bézout nous dit alors qu'il existe deux polynômes U, V dans $\mathbb{Q}[X]$ tels que $UP + VP' = 1$ et il est alors impossible de trouver z dans $\mathbb{C}$ tel que $P(z) = P'(z) = 0$.

2. Soit P un polynôme non constant dans $\mathbb{Q}[X]$ de degré n et $\alpha_1, \cdots, \alpha_n$ ses racines complexes.

   (a) Montrer que pour tout polynôme Q dans $\mathbb{Q}[X]$ le polynôme $R(X) = \prod_{j=1}^{n} Q(X + \alpha_j)$ est dans $\mathbb{Q}[X]$.
   Solution : Pour tout polynôme Q non nul de degré m dans $Q[X]$, on a :
   $$R(X) = \prod_{j=1}^{n} Q(X + \alpha_j) = \sum_{k=0}^{nm} b_k(\alpha_1, \cdots, \alpha_n) X^k,$$
   les b_k étant dans $\mathbb{Q}[X_1, \cdots, X_n]$. En remarquant que pour toute permutation σ de $\{1, \cdots, n\}$, on a :
   $$\sum_{k=0}^{nm} b_k\left(\alpha_{\sigma(1)}, \cdots, \alpha_{\sigma(n)}\right) X^k = \prod_{j=1}^{n} Q\left(X + \alpha_{\sigma(j)}\right) = R(X),$$
   on déduit que les b_k sont des polynômes symétriques, ils s'écrivent donc :
   $$b_k(\alpha_1, \cdots, \alpha_n) = c_k(\sigma_1, \cdots, \sigma_n),$$
   où les c_k sont dans $\mathbb{Q}[X_1, \cdots, X_n]$ et les σ_k sont les fonctions symétriques élémentaires des racines α_j.
   Avec :
   $$P(X) = a_n \prod_{j=1}^{n} (X - \alpha_j) = a_n \sum_{k=0}^{n} (-1)^k \sigma_k X^{n-k} \in Q[X],$$
   on déduit que les σ_k sont des nombres rationnels, il en est donc de même des $c_k(\sigma_1, \cdots, \sigma_n)$ et R est bien dans $\mathbb{Q}[X]$.

   (b) En supposant tous les α_j non nuls, montrer que pour tout polynôme Q dans $\mathbb{Q}[X]$ de degré m, le polynôme $S(X) = \prod_{j=1}^{n} \alpha_j^m Q\left(\frac{X}{\alpha_j}\right)$ est dans $\mathbb{Q}[X]$.
   Solution : Un raisonnement analogue nous montre que $S(X) = \prod_{j=1}^{n} \alpha_j^m Q\left(\frac{X}{\alpha_j}\right)$ est dans $\mathbb{Q}[X]$.

3. Soit α un nombre algébrique.

   (a) Montrer qu'il existe un unique polynôme unitaire P_α dans $\mathbb{Q}[X]$ tel que :
   $$\{P \in \mathbb{Q}[X] \mid P(\alpha) = 0\} = \mathbb{Q}[X] \cdot P_\alpha.$$
   On dit que P_α est le polynôme minimal de α et son degré est le degré de α. Il est noté $d(\alpha)$.
   Solution : Pour tout α dans $\mathbb{C}$, l'ensemble :
   $$\mathcal{I}_\alpha = \{P \in \mathbb{Q}[X] \mid P(\alpha) = 0\}$$
   est un idéal de l'anneau principal $\mathbb{Q}[X]$. Si α est algébrique, cet idéal n'est pas réduit à $\{0\}$ et il existe un unique polynôme unitaire non nul P_α dans $\mathbb{Q}[X]$ tel que $\mathcal{I}_\alpha = \mathbb{Q}[X] \cdot P_a$.

   (b) Montrer que le polynôme minimal de α est l'unique polynôme unitaire irréductible de $\mathbb{Q}[X]$ qui annule α.
   Solution : Par définition P_α est unitaire et annule α. Si $P_\alpha = QR$ avec Q, R dans $\mathbb{Q}[X]$, on a $Q(\alpha) R(\alpha) = 0$ et $Q(\alpha) = 0$ ou $R(\alpha) = 0$, ce qui équivaut à dire que Q ou R est dans l'idéal $\mathcal{I}_\alpha$. Ces polynômes étant de degré inférieur ou égal à celui de P_α, l'un des deux est nécessairement constant. On a donc ainsi prouvé que P_α est irréductible dans $\mathbb{Q}[X]$.
   Réciproquement si Q est un polynôme unitaire irréductible de $\mathbb{Q}[X]$ qui annule α, il est dans $\mathcal{I}_\alpha$, donc proportionnel à P_α et nécessairement égal à P_α puisque irréductible et unitaire. D'où l'unicité.

4. Montrer que l'ensemble $\mathbb{A}$ des nombres complexes algébriques est un corps.
Solution : Il s'agit de montrer que $\mathbb{A}$ est un sous corps de $\mathbb{C}$. On a bien $1 \in \mathbb{A}$ et il reste à montrer que si α, β sont dans $\mathbb{A}$ avec $\alpha \neq 0$, alors $\beta - \alpha$ et $\dfrac{\beta}{\alpha}$ sont aussi dans $\mathbb{A}$.
En notant P_α le polynôme minimal de α, $\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_n$ les racines complexes de P_α et P_β le polynôme minimal de β, le polynôme $Q(X) = \prod_{j=1}^{n} P_\beta(X + \alpha_j)$ est dans $\mathbb{Q}[X]$ et annule $\beta - \alpha$ et le polynôme $R(X) = \prod_{j=1}^{n} \alpha_j^m P_\beta\left(\dfrac{X}{\alpha_j}\right)$, où m est le degré de P_β, est dans $\mathbb{Q}[X]$ et annule $\alpha\beta$. Pour α non nul, $\dfrac{1}{\alpha}$ qui est annulé par $X^n P_\alpha\left(\dfrac{1}{X}\right) \in \mathbb{Q}[X]$ est algébrique.

5. Soit $(P_k)_{1 \leq k \leq n}$ une famille de polynômes unitaires non constants dans $\mathbb{Q}[X]$. Pour tout k compris entre 1 et n, on note p_k le degré de P_k et $\alpha_{k,1}, \cdots, \alpha_{k,p_k}$ les racines complexes de P_k. Montrer que le polynôme Q défini par :

$$Q(X) = \prod_{\substack{1 \leq j_1 \leq p_1 \\ \vdots \\ 1 \leq j_n \leq p_n}} \left(X^n + \alpha_{1,j_1} X^{n-1} + \cdots + \alpha_{n-1,j_{n-1}} X + \alpha_{n,j_n}\right)$$

est dans $\mathbb{Q}[X]$.
Solution : Le polynôme Q est de degré $np_1 \cdots p_n$ et ses coefficients sont des fonctions polynomiales à coefficients entiers des α_{k,j_k}. Une permutation de l'ensemble d'indices $\{1, \cdots, p_k\}$ ne modifiant pas les polynôme Q, ces coefficients sont des sommes et produits des fonctions symétriques élémentaires des racines de chaque P_k, ils sont donc rationnels.

6. En utilisant la question précédente, montrer que le corps $\mathbb{A}$ des nombres complexes algébriques est algébriquement clos.
Solution : Soit P un polynôme non constant à coefficients dans $\mathbb{A}$. Ce polynôme a des racines complexes et il s'agit de montrer que toutes ces racines sont algébriques. Comme $\mathbb{A}$ est un corps, on peut supposer P unitaire. On l'écrit sous la forme :

$$P(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n$$

les coefficients a_k étant algébriques.
On désigne par α une racine complexe de P. Pour tout k compris entre 1 et n on note P_k le polynôme minimal de a_k et $\alpha_{k,1} = a_k, \alpha_{k,2}, \cdots, \alpha_{k,n_k}$ les racines complexes de P_k.
Le polynôme $Q(X) = \prod_{\substack{1 \leq j_1 \leq p_1 \\ \vdots \\ 1 \leq j_n \leq p_n}} \left(X^n + \alpha_{1,j_1} X^{n-1} + \cdots + \alpha_{n-1,j_{n-1}} X + \alpha_{n,j_n}\right)$ est alors dans $\mathbb{Q}[X]$ et annule α puisque le multi-indice $(j_1, \cdots, j_n) = (1, \cdots, 1)$ donne le polynôme P.

7. Soient α, β deux nombres algébriques, $P_\alpha(X) = \sum_{k=0}^{n} a_k X^k$ le polynôme minimal de α et $P_\beta(X) = \sum_{k=0}^{m} b_k X^k$ celui de β avec $a_n = b_m = 1$. On note :

$$\left\{\alpha^i \beta^j \mid 0 \leq i \leq n-1,\ 0 \leq j \leq m-1\right\} = \{\gamma_k \mid 1 \leq k \leq p\}$$

où $p = nm$ et $\gamma_1 = \alpha^0 \beta^0 = 1$. On désigne par v le vecteur de $\mathbb{C}^p$ de composantes $\gamma_1, \cdots, \gamma_p$.

   (a) Montrer qu'il existe deux matrices carrées d'ordre p à coefficients rationnels A et B telles que $\alpha v = Av$ et $\beta v = BV$.
   Solution : Pour tout entier k compris entre 1 et p il existe deux indices i, j tels que

$\gamma_k = \alpha^i\beta^j$ et $\alpha\gamma_k = \alpha^{i+1}\beta^j$. Pour i compris entre 0 et $n-2$, $\alpha\gamma_k$ est l'un des γ_r et pour $i = n-1$, on a :

$$\alpha\gamma_k = \alpha^n\beta^j = -\sum_{r=0}^{n-1} a_r\alpha^r\beta^j$$

qui est une combinaison linéaire à coefficients rationnels des $\gamma_1, \cdots, \gamma_p$. Il existe donc une matrice A dans $\mathcal{M}_p(\mathbb{Q})$ telle que $\alpha v = Av$.
De manière analogue, on voit qu'il existe une matrice B dans $\mathcal{M}_p(\mathbb{Q})$ telle que $\beta v = Bv$.

(b) En utilisant le résultat de **II.7a**, retrouver le fait que $\mathbb{A}$ est un corps.
Solution : Pour α, β dans $\mathbb{A}$, on a avec les notations précédentes, $(A-B)\,v = (\alpha-\beta)\,v$ avec v non nul dans $\mathbb{C}^p$, ce qui signifie que $\alpha-\beta$ est une valeur propre de la matrice $A-B$, c'est donc une racine du polynôme caractéristique χ_{A-B} qui est dans $\mathbb{Q}[X]$ puisque $A-B$ est une matrice à coefficients rationnels. Il en résulte que $\alpha-\beta$ est algébrique. De même avec $(AB)\,v = (\alpha\beta)\,v$ on déduit que $\alpha\beta$ est algébrique.
Pour α non nul, $\dfrac{1}{\alpha}$ qui est annulé par $X^n P_\alpha\left(\dfrac{1}{X}\right) \in \mathbb{Q}[X]$ est algébrique. Avec $0, 1$ algébriques on en déduit que $\mathbb{A}$ est un sous-corps de $\mathbb{C}$.

8. Soit $P(X) = \sum_{k=0}^{n} a_k X^k$ un polynôme non constant de degré n à coefficients dans le corps $\mathbb{A}$ et α une racine complexe de P. Pour tout entier k compris entre 0 et n on note n_k le degré du nombre algébrique a_k et :

$$\left\{\alpha^i a_0^{i_0} a_1^{i_1}\cdots a_n^{i_n} \mid 0 \le i \le n-1,\ 0 \le i_k \le n_k - 1\right\} = \{\gamma_k \mid 1 \le k \le p\}$$

où $p = nn_0\cdots n_n$ et $\gamma_1 = 1$. On désigne par v le vecteur de $\mathbb{C}^p$ de composantes $\gamma_1, \cdots, \gamma_p$.

(a) Montrer qu'il existe une matrice carrée d'ordre p à coefficients rationnels A telle que $\alpha v = Av$.
Solution : Pour tout entier k compris entre 1 et p il existe un multi-indice $(i, i_0, \cdots, i_n)$ tel que $\alpha\gamma_k = \alpha^{i+1} a_0^{i_0} a_1^{i_1}\cdots a_n^{i_n}$. Pour i compris entre 0 et $n-2$, $\alpha\gamma_k$ est l'un des γ_r et pour $i = n-1$, on a :

$$\alpha\gamma_k = \alpha^n a_0^{i_0} a_1^{i_1}\cdots a_n^{i_n} = -\sum_{r=0}^{n-1} a_r\alpha^r a_0^{i_0} a_1^{i_1}\cdots a_n^{i_n}$$

avec :

$$a_r\alpha^r a_0^{i_0} a_1^{i_1}\cdots a_n^{i_n} = \alpha^r a_r^{i_r+1}\prod_{j\neq r} a_j^{i_j}.$$

Pour $i_r \le n_r - 2$ ce coefficient est l'un des γ_s et pour $i_r = n_r - 1$ c'est une combinaison linéaire à coefficients rationnels des $\gamma_1, \cdots, \gamma_p$ puisque a_r est algébrique de degré n_r. Il existe donc une matrice A dans $\mathcal{M}_p(\mathbb{Q})$ telle que $\alpha v = Av$.

(b) En déduire que α est algébrique. On retrouve ainsi le fait que $\mathbb{A}$ est algébriquement clos.
Solution : Ce qui précède nous dit que α est une valeur propre de la matrice $A \in \mathcal{M}_p(\mathbb{Q})$, c'est donc une racine du polynôme caractéristique χ_A qui est dans $\mathbb{Q}[X]$ et α est algébrique.

– III – Nombres transcendants et automorphismes croissants de $\mathbb{Q}^{+,*}$

$\mathbb{R}$ et $\mathbb{C}$ sont munis de leur structure naturelle de $\mathbb{Q}$-espace vectoriel.

$\mathbb{R}^{+,*}$ désigne le groupe multiplicatif des réels strictement positifs.

Si α et β sont deux nombres complexes avec α non nul, on définit alors α^β par $\alpha^\beta = e^{(\ln(a)+i\pi)\beta}$ si $\alpha = -a$ avec a réel strictement positif et $\alpha^\beta = e^{\beta\ln(\alpha)}$ où ln est la détermination principale du logarithme si α est dans $\mathbb{C}\setminus\mathbb{R}^-$.

On admettra les résultats suivants.

Théorème 1 (des six exponentielles) *Si x_1, x_2 sont deux nombres complexes linéairement indépendants sur $\mathbb{Q}$ et y_1, y_2, y_3 trois nombres complexes linéairement indépendants sur $\mathbb{Q}$, alors l'un au moins des six nombres complexes $e^{x_i y_j}$, pour $1 \leq i \leq 2$ et $1 \leq j \leq 3$, est transcendant.*

Théorème 2 (Gelfond-Schneider) *Si α est un nombre algébrique non nul et β un nombre algébrique n'appartenant pas à $\mathbb{Q}$, alors α^β est transcendant.*

1. Montrer que les seuls endomorphismes du groupe additif $\mathbb{R}$ qui sont monotones sont les homothéties (i.e. les applications $x \mapsto \lambda x$, où λ est une constante réelle).
   Solution : Un endomorphisme du groupe additif $\mathbb{R}$ est une application $f : \mathbb{R} \to \mathbb{R}$ qui vérifie l'équation fonctionnelle de Cauchy :

$$\forall (x, y) \in \mathbb{R}^2, \quad f(x+y) = f(x) + f(y). \tag{2}$$

   (a) On montre tout d'abord que si f est un endomorphisme du groupe additif $\mathbb{R}$, alors :

$$\forall a \in \mathbb{R}, \quad \forall r \in \mathbb{Q}, \quad f(ra) = rf(a).$$

   En prenant $(x, y) = (0, 0)$ dans (**??**), on obtient $f(0) = 2f(0)$, ce qui équivaut à $f(0) = 0$ (un morphisme de groupes transforme le neutre en neutre).
   En prenant $(x, y) = (x, -x)$ dans (**??**), on obtient $f(x) + f(-x) = 0$. On a donc $f(-x) = -f(x)$ pour tout $x \in \mathbb{R}$, c'est-à-dire que la fonction f est impaire (un morphisme de groupes transforme l'opposé en opposé).
   De (**??**) on déduit par récurrence que pour tout $a \in \mathbb{R}$ on a :

$$\forall n \in \mathbb{N}, \quad f(na) = nf(a).$$

   En effet, le résultat est vrai pour $n = 0$ et le supposant vrai pour $n \geq 0$, on a :

$$f((n+1)a) = f(na) + f(a) = nf(a) + f(a) = (n+1)f(a),$$

   il est donc vrai pour tout $n \in \mathbb{N}$.
   En écrivant, pour tout $n \in \mathbb{N} \setminus \{0\}$, que $f(a) = f\left(n\frac{a}{n}\right) = nf\left(\frac{a}{n}\right)$, on déduit que $f\left(\frac{a}{n}\right) = \frac{1}{n} f(a)$ pour tout $a \in \mathbb{R}$ et tout $n \in \mathbb{N} \setminus \{0\}$. Il en résulte que pour tout rationnel positif $r = \frac{p}{q}$, avec $p \in \mathbb{N}$ et $q \in \mathbb{N} \setminus \{0\}$, on a :

$$f(ra) = f\left(p\frac{a}{q}\right) = pf\left(\frac{a}{q}\right) = \frac{p}{q} f(a) = rf(a).$$

   Enfin avec l'imparité de f, on déduit que ce dernier résultat est encore vrai pour les rationnels négatifs. On a donc $f(ra) = rf(a)$ pour tout $a \in \mathbb{R}$ et tout $r \in \mathbb{Q}$.

   (b) Soit f un endomorphisme croissant du groupe additif $\mathbb{R}$. En particulier, on a $\lambda = f(1) \geq f(0) = 0$.
   En désignant, pour $x \in \mathbb{R}$, par $(r_n)_{n\in\mathbb{N}}$ et $(s_n)_{n\in\mathbb{N}}$ des suites d'approximations décimales par défaut et par excès de ce réel, on a pour tout $n \in \mathbb{N}$:

$$\lambda r_n = f(r_n) \leq f(x) \leq f(s_n) = \lambda s_n$$

   et faisant tendre n vers l'infini, on en déduit que $f(x) = \lambda x$.

   (c) On procède de manière analogue pour f décroissante.

2. Montrer que l'identité est le seul endomorphisme de corps non identiquement nul de $\mathbb{R}$.
Solution : Si f est endomorphisme du corps $\mathbb{R}$, on a alors $f(x+y) = f(x) + f(y)$ et $f(xy) = f(x) f(y)$ pour tous x, y dans $\mathbb{R}$.
Avec $f(1) = (f(1))^2$, on déduit que $f(1) = 0$ ou $f(1) = 1$. Si $f(1) = 0$, alors pour tout $x \in \mathbb{R}$ on a $f(x) = f(x) f(1) = 0$ et f est identiquement nulle. C'est une homothétie de rapport 0.
On suppose donc que f n'est pas identiquement nulle et on a alors $f(1) = 1$.
Avec $f(x^2) = (f(x))^2 \geq 0$, on déduit que $f(x) \geq 0$ pour tout $x \geq 0$ et pour $x \geq y$ dans $\mathbb{R}$, on a $f(x) - f(y) = f(x-y) \geq 0$, ce qui signifie que f est croissante. On déduit alors du résultat précédent que $f(x) = x$ pour tout $x \in \mathbb{R}$ ($\lambda = f(1) = 1$). L'identité est donc le seul morphisme de corps non identiquement nul de $\mathbb{R}$ dans lui même.

3. Soient G, H deux sous-groupes du groupe additif $\mathbb{R}$ et φ un morphisme de groupes croissant de G vers H. Montrer qu'il existe un réel positif λ tel que $\varphi(x) = \lambda x$ pour tout x dans G.
Solution : Si $G = \{0\}$ alors $\varphi(0) = 0$ et $\lambda = 0$ convient.
Si G n'est pas réduit à $\{0\}$, alors l'ensemble $G \cap \mathbb{R}^{+,*}$ est non vide du fait que pour tout x non nul dans G, $-x$ est aussi dans G.
Supposons qu'il existe a dans $G \cap \mathbb{R}^{+,*}$ tel que $\varphi(a) = 0$. Pour tout x dans $G \cap \mathbb{R}^{+,*}$ on peut trouver un entier naturel n tel que $x < na$ ($\mathbb{R}$ est archimédien) et avec la croissance de φ, on déduit que :
$$0 \leq \varphi(x) \leq \varphi(na) = n\varphi(a) = 0,$$
c'est-à-dire que φ est nul sur $G \cap \mathbb{R}^{+,*}$. Avec $\varphi(-x) = -\varphi(x)$ pour tout x dans G, on déduit que φ est le morphisme nul et $\lambda = 0$ convient.
Si pour tout x dans $G \cap \mathbb{R}^{+,*}$, on a $\varphi(x) \neq 0$, avec la croissance de φ on déduit que $\varphi(x) > 0$ pour tout x dans $G \cap \mathbb{R}^{+,*}$. Supposons qu'il existe $a \neq b$ dans $G \cap \mathbb{R}^{+,*}$ tels $\dfrac{a}{b} \neq \dfrac{\varphi(a)}{\varphi(b)}$. On peut supposer que $\dfrac{a}{b} < \dfrac{\varphi(a)}{\varphi(b)}$ et avec la densité de $\mathbb{Q}$ dans $\mathbb{R}$ on déduit qu'il existe un nombre rationnel $\dfrac{p}{q}$ tel que $\dfrac{a}{b} < \dfrac{p}{q} < \dfrac{\varphi(a)}{\varphi(b)}$. On a alors $qa < pb$ et avec la croissance de φ on déduit que $q\varphi(a) \leq p\varphi(b)$, ce qui est en contradiction avec $\dfrac{p}{q} < \dfrac{\varphi(a)}{\varphi(b)}$. La fonction $x \mapsto \dfrac{\varphi(x)}{x}$ est donc constante sur $G \cap \mathbb{R}^{+,*}$. En notant λ cette constante on a $\lambda \geq 0$ et $\varphi(x) = \lambda x$ pour tout x dans $G \cap \mathbb{R}^{+,*}$, ce qui entraîne $\varphi(x) = \lambda x$ pour tout x dans G puisque φ est un morphisme de groupes. On peut remarquer que λ est nulle si, et seulement si, φ est le morphisme nul.
Pour $G = H = \mathbb{R}$ on retrouve le résultat de la question **III.??.**

4. Soient G, H deux sous-groupes du groupe multiplicatif $\mathbb{R}^{+,*}$ et σ un morphisme de groupes croissant de G vers H. Montrer qu'il existe un réel positif λ tel que $\sigma(x) = x^\lambda$ pour tout x dans G.
Solution : Si $G = \{1\}$, alors $\sigma(1) = 1$ et $\lambda = 1$ convient.
Sinon $\ln(G) = \{\ln(x) \mid x \in G\}$ est un sous-groupe du groupe additif $\mathbb{R}$ non réduit à $\{0\}$ et $\varphi : t \mapsto \ln(\sigma(e^t))$ est un morphisme de groupes croissant de $\ln(G)$ vers $\ln(H)$ (la fonction logarithme est un morphisme de groupes strictement croissant de $(\mathbb{R}^{+,*}, \times)$ sur $(\mathbb{R}, +)$). Il existe donc un réel $\lambda \geq 0$ tel que $\varphi(t) = \lambda t$ pour tout t dans $\ln(G)$. On a donc $\sigma(e^t) = e^{\lambda t}$ pour tout t dans $\ln(G)$ et pour tout x dans G, on a $\sigma(x) = \sigma\left(e^{\ln(x)}\right) = e^{\lambda \ln(x)} = x^\lambda$.
On peut remarquer que λ est nulle si, et seulement si, σ est l'application constante égale à 1.

5. Montrer que les réels $\ln(2)$, $\ln(3)$ et $\ln(5)$ sont linéairement indépendants sur $\mathbb{Q}$.
Solution : Supposons qu'il existe des nombres rationnels r_1, r_2, r_3 tels que $r_1 \ln(2) + r_2 \ln(3) + r_3 \ln(5) = 0$. En réduisant au même dénominateur, on peut écrire chaque r_j sous la forme $r_j = \dfrac{n_j}{d}$ où les n_j et d sont des entiers relatifs et on a $n_1 \ln(2) + n_2 \ln(3) + n_3 \ln(5) = 0$. En prenant l'exponentielle des deux membres de cette égalité, on a $2^{n_1} 3^{n_2} 5^{n_3} = 1$ et l'unicité de la

décomposition en facteurs premiers impose que $n_1 = n_2 = n_3 = 0$. Les r_j sont donc tous nuls pour $j = 1, 2, 3$.

6. En utilisant le théorème des six exponentielles, montrer que si α est un nombre complexe tel que 2^α, 3^α et 5^α sont des entiers alors α est un entier.
Solution : On note $x_1 = 1$, $x_2 = \alpha$ et $y_1 = \ln(2)$, $y_2 = \ln(3)$, $y_3 = \ln(5)$.
Si α n'est pas rationnel, alors les hypothèses du théorème des six exponentielles sont vérifiées et l'un des six réels $e^{x_i y_j}$ est transcendant, ce qui équivaut à dire que l'un des trois réels 2^α, 3^α ou 5^α est transcendant, ils ne peuvent donc être entiers.
Si 2^α, 3^α et 5^α sont entiers, α est donc nécessairement rationnel. Notons $\alpha = \dfrac{p}{q}$ avec p, q entiers premiers entre eux. Comme $2^{\frac{p}{q}}$ est entier, on a $2^p = m^q$ avec m entier naturel. L'unicité de la décomposition en facteurs premiers nous dit que m est nécessairement une puissance de 2 et $2^p = 2^{rq}$ avec r entier entraîne $p = rq$ et $q = 1$ puisque p et q sont premiers entre eux. En définitive α est un entier.

7. Soit α un nombre algébrique différent de 0 et de 1. Montrer que si β est un nombre complexe n'appartenant pas à $\mathbb{Q}$ alors l'un des trois nombres complexes α^β, α^{β^2} ou α^{β^3} est transcendant.
Solution : Si β est algébrique, comme il n'appartient pas à $\mathbb{Q}$, le théorème de Gelfond-Schneider nous dit que α^β est transcendant.
On suppose que β n'est pas algébrique. Dans ce cas les nombres complexes $y_1 = \ln(\alpha)$, $y_2 = \beta \ln(\alpha)$ et $y_3 = \beta^2 \ln(\alpha)$ sont indépendants sur $\mathbb{Q}$. En effet, si il existe des rationnels r_j tels que $\sum_{j=1}^{3} r_j y_j = 0$, tenant compte de $\ln(\alpha) \neq 0$ (α est différent de 1), on a alors $r_1 + r_2\beta + r_3\beta^2 = 0$ et les r_j sont nécessairement tous nuls puisque β n'est pas algébrique.
En posant $x_1 = 1$, $x_2 = \beta$, les hypothèses du théorème des six exponentielles sont vérifiées et l'un des six nombres complexes $e^{x_i y_j}$ est transcendant, ce qui équivaut à dire que l'un des quatre nombres α, α^β, α^{β^2}, α^{β^3} est transcendant, encore équivalent à dire que l'un des trois nombres α^β, α^{β^2}, α^{β^3} est transcendant puisque α est algébrique.

8. Soit G un sous-groupe du groupe multiplicatif $\mathbb{R}^{+,*}$ contenu dans $\mathbb{A}$. Montrer que si σ est un automorphisme croissant de G alors il existe un nombre rationnel positif r tel que $\sigma(x) = rx$ pour tout x dans G.
Solution : Si $G = \{1\}$, alors $\sigma(1) = 1$ et $r = 1$ convient.
Sinon on a vu qu'il existe un réel positif r tel que $\sigma(x) = x^r$ pour tout x dans G et comme σ est un automorphisme de $G \neq \{1\}$, on a nécessairement $r > 0$.
Comme G est contenu dans $\mathbb{A}$, pour tout $\alpha \neq 1$ dans G on a $\sigma(\alpha) = \alpha^r \in \mathbb{A}$, $\sigma^2(\alpha) = \alpha^{r^2} \in \mathbb{A}$ et $\sigma^3(\alpha) = \alpha^{r^3} \in \mathbb{A}$ avec $\alpha \in \mathbb{A}$. On déduit alors de la question précédente que r est rationnel.

9. Soit P un polynôme non constant à coefficients entiers relatifs défini par $P(X) = \sum_{k=0}^{n} a_k X^k$ avec a_n non nul.

   (a) Montrer que si $r = \dfrac{p}{q}$ est une racine rationnelle non nulle de P, où p, q sont deux entiers relatifs premiers entre eux, alors p divise a_0 et q divise a_n.
   Solution : Si $P(r) = 0$, alors $q^n P(r) = a_0 q^n + a_1 p q^{n-1} + \cdots + a_{n-1} p^{n-1} q + a_n p^n = 0$ et avec p, q premiers entre eux on déduit du théorème de Gauss que p divise a_0 et q divise a_n.

   (b) Montrer que si $P(X) = \sum_{k=0}^{n} a_k X^k$ est un polynôme unitaire non constant à coefficients entiers relatifs ($a_n = 1$) alors les racines de P sont soit entières, soit irrationnelles.
   Solution : Si $r = \dfrac{p}{q}$ est une racine rationnelle non nulle de P, où p, q sont deux entiers relatifs premiers entre eux avec $q > 0$, alors q qui divise $a_n = 1$ est nécessairement égal à 1 et r est entier.

(c) Montrer que pour tout entier $r \geq 2$ et tout nombre premier $p \geq 2$, $\sqrt[r]{p}$ est irrationnel.
Solution : $\sqrt[r]{p}$ est racine de $P(X) = X^r - p = 0$ et $\sqrt[r]{p}$ n'étant pas entier ($\sqrt[r]{p} = m \in \mathbb{N}$ entraîne $m \geq 2$ et $p = m^r$ ne peut être premier) est nécessairement irrationnel.

10. Montrer que l'identité est le seul automorphisme croissant du groupe multiplicatif $\mathbb{Q}^{+,*}$ (théorème de Glass-Ribenboim, 1993).
Solution : Soit σ automorphisme croissant du groupe multiplicatif $\mathbb{Q}^{+,*}$. D'après la question **III.8** il existe un rationnel $r = \dfrac{p}{q}$ avec p, q entiers naturels non nuls premiers entre eux tels que $\sigma(x) = x^r$ pour tout x dans $\mathbb{Q}^{+,*}$. En particulier, on a $\sigma(2) = 2^{\frac{p}{q}} = \dfrac{n}{m}$ avec n, m entiers naturels non nuls premiers entre eux. On a donc $2^p m^q = n^q$, ce qui implique que $m = 1$ (théorème de Gauss) et n est une puissance de 2 (unicité de la décomposition en facteurs premiers), soit $n = 2^s$ et $2^p = 2^{qs}$, ce qui donne $p = qs$ et $q = 1$ puisque p et q sont premiers entre eux. On a donc $r = p \in \mathbb{N}^*$. D'autre part, on a $\sigma^{-1}(x) = \sqrt[p]{x} \in \mathbb{Q}^{+,*}$ pour tout $x \in \mathbb{Q}^{+,*}$, donc $\sigma^{-1}(2) = \sqrt[p]{2} \in \mathbb{Q}^{+,*}$ et nécessairement $p = 1$.