CORRIGÉ DU DS N°1

PROBLÈME 1

Question préliminaire :

• $\forall p \in \mathcal{P}(E),\ p\mathbf{o}p = p$ donc $p\mathcal{R}p$. $\mathcal{R}$ est reflexive.
• $(p\mathcal{R}q$ et $q\mathcal{R}p) \Longrightarrow (p\mathbf{o}q = q\mathbf{o}p = p$ et $q\mathbf{o}p = p\mathbf{o}q = q) \Longrightarrow p = q$. $\mathcal{R}$ est antisymétrique.
• $(p\mathcal{R}q$ et $q\mathcal{R}r) \Longrightarrow (p\mathbf{o}q = q\mathbf{o}p = p$ et $q\mathbf{o}r = r\mathbf{o}q = q) \Longrightarrow p\mathbf{o}r = (p\mathbf{o}q)\mathbf{o}r = p\mathbf{o}(q\mathbf{o}r) = p\mathbf{o}q = p$ et, de même, $r\mathbf{o}p = p$. $\mathcal{R}$ est transitive.
Donc $\mathcal{R}$ est une relation d'ordre sur $\mathcal{P}(E)$.

Première partie :

1°) a) On a $f\mathbf{o}g = g\mathbf{o}f$ donc,si $y \in \mathrm{Im}f$ avec $y = f(z)$, on a $g(y) = g[f(z)] = f[g(z)] \in \mathrm{Im}f$ et, si $x \in \mathrm{Ker}f$, $f[g(x)] = g[f(x)] = g(0) = 0$.
Donc $\mathrm{Im}f$ et $\mathrm{Ker}f$ sont stables par g .

b) Soit $x \in E$, x s'écrit $x = x_1 + x_2$ avec $x_1 \in \mathrm{Im}f$ et $x_2 \in \mathrm{Ker}f$ car $f \in \mathcal{P}(E)$ et on a $\varphi_g(f)(x = (f\mathbf{o}g)(x) - (g\mathbf{o}f)(x) = f\big((g(x_1) + g(x_2)\big) - g(x_1) = f\big(g(x_1)\big) - g(x_1) = g(x_1) - g(x_1) = 0$ car $g(x_1) \in \mathrm{Im}f$ et $g(x_2) \in \mathrm{Ker}f$ et que $\mathrm{Im}f$ est aussi le sous-espace vectoriel des vecteurs invariants par f (cf cours).
Donc $f \in \mathcal{P}(E)$ et $\mathrm{Im}f$ et $\mathrm{Ker}f$ stables par g impliquent $\varphi_g(f) = 0$.

2°) a) • $(f\mathbf{o}g)\mathbf{o}(f\mathbf{o}g) = f\mathbf{o}(g\mathbf{o}f)\mathbf{o}g = f\mathbf{o}(f\mathbf{o}g)\mathbf{o}g = (f\mathbf{o}f)\mathbf{o}(g\mathbf{o}g) = f\mathbf{o}g$
donc $f\mathbf{o}g \in \mathcal{P}(E)$.
• $(f + g - f\mathbf{o}g)\mathbf{o}(f + g - f\mathbf{o}g) = f^2 + f\mathbf{o}g - f^2\mathbf{o}g + g\mathbf{o}f + g^2 - g\mathbf{o}f\mathbf{o}g - f\mathbf{o}g\mathbf{o}f - f\mathbf{o}g^2 + (f\mathbf{o}g)\mathbf{o}(f\mathbf{o}g)$
$= f + f\mathbf{o}g - f\mathbf{o}g + g - f\mathbf{o}g^2 - f^2\mathbf{o}g - f\mathbf{o}g + f\mathbf{o}g$
$= f + g - f\mathbf{o}g$
donc $(f + g - f\mathbf{o}g) \in \mathcal{P}(E)$.

b) • Puisque $f\mathbf{o}g = g\mathbf{o}f$, f et g jouent le même rôle et il suffit de montrer les résultats pour f.
• Cette commutativité donne $f\mathbf{o}(f\mathbf{o}g) = (f\mathbf{o}g)\mathbf{o}f$ et $f\mathbf{o}(f + g - f\mathbf{o}g) = (f + g - f\mathbf{o}g)\mathbf{o}f$.
Or $f^2\mathbf{o}g = f\mathbf{o}g$ et $f\mathbf{o}(f + g - f\mathbf{o}g) = f^2 + f\mathbf{o}g - f^2\mathbf{o}g = f$.
Donc $(f\mathbf{o}g)\mathcal{R}f,\quad (f\mathbf{o}g)\mathcal{R}g,\quad f\mathcal{R}(f + g - f\mathbf{o}g),\quad g\mathcal{R}(f + g - f\mathbf{o}g)$.

c) • Montrons que $m = (f\mathbf{o}g)$ est la borne inférieure de $\{f, g\}$ dans $\mathcal{P}(E)$.
◇ $(f\mathbf{o}g) \in \mathcal{P}(E)$ (cf. ci-dessus).
◇ $(f\mathbf{o}g)\mathcal{R}f,\quad (f\mathbf{o}g)\mathcal{R}g$ (cf. ci-dessus).
◇ Si $q \in \mathcal{P}(E)$ et $q\mathcal{R}f,\ q\mathcal{R}g$ on a $q\mathbf{o}(f\mathbf{o}g) = (q\mathbf{o}f)\mathbf{o}g = q\mathbf{o}g = q$ et, de même, $(f\mathbf{o}g)\mathbf{o}q = q$ donc $q\mathcal{R}(f\mathbf{o}g)$.
• Montrons que $M = (f + g - f\mathbf{o}g)$ est la borne supérieure de $\{f, g\}$ dans $\mathcal{P}(E)$.
◇ $(f + g - f\mathbf{o}g) \in \mathcal{P}(E)$.
◇ $f\mathcal{R}(f + g - f\mathbf{o}g),\quad g\mathcal{R}(f + g - f\mathbf{o}g)$.
◇ Si $q \in \mathcal{P}(E)$ et $f\mathcal{R}q,\ g\mathcal{R}q$ on a $q\mathbf{o}(f+g-f\mathbf{o}g) = q\mathbf{o}f+q\mathbf{o}g-(q\mathbf{o}f)\mathbf{o}g = f+g-f\mathbf{o}g = q$ et, de même, $(f + g - f\mathbf{o}g)\mathbf{o}q = (f + g - f\mathbf{o}g)$ donc $(f + g - f\mathbf{o}g)\mathcal{R}q$.

Seconde partie :

1°) a) Montrons, par récurrence sur k, que $\underline{\forall k \in \mathbb{N}^*, \quad f^k \mathbf{o} g - g \mathbf{o} f^k = \alpha\, k\, f^k}$:
◇ Pour $k = 1$, c'est l'hypothèse.
◇ Si le résultat est vérifié pour k on a :

$$\begin{aligned} f^{k+1}\mathbf{o}g - g\mathbf{o}f^{k+1} &= f\mathbf{o}(f^k\mathbf{o}g) - g\mathbf{o}f^{k+1} = f\mathbf{o}\big(g\mathbf{o}f^k + \alpha\, k\, f^k\big) - g\mathbf{o}f^{k+1} \\ &= f\mathbf{o}g\mathbf{o}f^k - g\mathbf{o}f\mathbf{o}f^k + \alpha\, k\, f^{k+1} = \big(f\mathbf{o}g - g\mathbf{o}f\big)\mathbf{o}f^k + \alpha\, k\, f^{k+1} \\ &= (\alpha f)\mathbf{o}f^k + \alpha\, k\, f^{k+1} = \alpha(k+1)f^{k+1} \quad \text{cqfd.} \end{aligned}$$

b) On suppose donc que : $\forall k \in \mathbb{N}^*,\ f^k \neq 0$. Pour montrer que la famille $(f^k)_{kn\mathbb{N}^*}$ est une famille libre, il suffi de montrer que, pour tout $n \in \mathbb{N}^*$, la famille $(f^k)_{1 \leqslant k \leqslant n}$ est libre.
Pour cela, on procède par récurrence sur n.
◇ Pour $n = 1$, cela résulte de $f \neq 0$.
◇ Supposons donc le résultat vérifié à l'ordre n, et soit $\lambda_0, \lambda_1, \ldots, \lambda_{n+1}$ $n+1$ scalaires tels que $\displaystyle\sum_{k=1}^{n+1} \lambda_k f^k = 0$. En appliquant φ_g, compte tenu de la linéarité de φ_g et des résultats précédents (qui s'écrivent $\varphi_g(f^k) = \alpha k f^k$), on obtient : $\displaystyle\sum_{k=1}^{n+1} \alpha k \lambda_k f^k = 0$. En soustrayant à cette égalité $\alpha(n+1)$-fois la précédente, on obtient : $\displaystyle\sum_{k=1}^{n} \alpha(k-(n+1))\lambda_k f^k = 0$; d'après l'hypothèse de récurrence, on a alors : $\forall k \in [\![1, n]\!],\ \alpha(k-(n+1))\lambda_k = 0$ d'où $\lambda_k = 0$ puisque $\alpha \neq 0$. On en déduit ensuite $\lambda_{n+1} = 0$ puisque $f^{n+1} \neq 0$, ce qui démontre que la famille $(f^k)_{1 \leqslant k \leqslant n+1}$ est libre. CQFD.

c) La conclusion est immédiate : E étant de dimension finie ne peut contenir de famille libre infinie. Donc $\exists k \in \mathbb{N}^*,\ f^k = 0$ c'est à dire que $\underline{f \text{ est nilpotente}}$.

d) Si on suppose de plus $f \in \mathcal{P}(E)$, alors $f^2 = f$ puis par récurrence $f^k = f$ pour tout entier $k \in \mathbb{N}^*$, d'où $\underline{f = 0}$.

2°) a) i) On a $f\mathbf{o}g - g\mathbf{o}f = \alpha f + \beta g$. Composons cette égalité à droite et à gauche par g, on obtient :
$f\mathbf{o}g - g\mathbf{o}f\mathbf{o}g = \alpha f\mathbf{o}g + \beta g$ et $g\mathbf{o}f\mathbf{o}g - g\mathbf{o}f = \alpha g\mathbf{o}f + \beta g$.
Donc, en additionnant les résultats obtenus, $f\mathbf{o}g - g\mathbf{o}f = \alpha\big(f\mathbf{o}g + g\mathbf{o}f\big) + 2\beta g$.
D'où : $\alpha f + \beta g = \alpha\big(f\mathbf{o}g - g\mathbf{o}f + 2g\mathbf{o}f\big) + 2\beta g$
$= \alpha\big(\alpha f + \beta g + 2g\mathbf{o}f\big) + 2\beta g$
$= \alpha^2 f + \beta(\alpha+2)g + 2\alpha g\mathbf{o}f$
Donc $\underline{2\alpha g\mathbf{o}f + \beta(\alpha+1)g = \alpha(1-\alpha)f}$.

ii) • Donc $\forall x \in E,\ f(x) = g\left[\dfrac{2\alpha f(x) + \beta(\alpha+1)x}{\alpha(1-\alpha)}\right]$ car $\alpha(1-\alpha) \neq 0$ et donc $\underline{\mathrm{Im}f \subset \mathrm{Im}g}$.
• Mais alors $\forall x \in E,\ g[f(x)] = f(x)$ car $f(x) \in \mathrm{Im}g$ donc $\underline{g\mathbf{o}f = f}$.

iii) • Soit $x \in \mathrm{Im}f,\ x \neq 0$ (un tel x existe car $f \neq 0$). On a $x \in \mathrm{Im}g$ donc $\big(f\mathbf{o}g - g\mathbf{o}f\big)(x) = \alpha f(x) + \beta g(x) \Leftrightarrow f(x) - g(x) = x - x = \alpha x + \beta x$ donc $\underline{\alpha + \beta = 0}$.
• D'après l'égalité obtenue en **(i)**, en remplaçant $g\mathbf{o}f$ par f et β par $-\alpha$, on a $\alpha(\alpha+1)\big(g - f\big) = 0$ d'où, puisque $g \neq f$, $\underline{\alpha = -1}$.

• Donc $f\mathbf{o}g - g\mathbf{o}f = -f + g$ et $g\mathbf{o}f = f$ donc $f\mathbf{o}g = g$ donc $\forall x \in E$, $g(x) = f[g(x)]$ et $\text{Im}g \subset \text{Im}f$ puis finalement $\underline{\text{Im}g = \text{Im}f}$.

iv) Soient f, g des projecteurs tels que $g\mathbf{o}f = f$ et $\text{Im}g \subset \text{Im}f$. Alors, $\forall x \in E,\ f[g(x)] = g(x)$ car $g(x) \in \text{Im}f$ donc $f\mathbf{o}g = g$ d'où $\underline{\varphi_g(f) = -f + g}$.

b) i) • Si $\alpha \neq 1$, on peut appliquer le résultat de la question précédente, d'où $\alpha = -1$, ce qui est exclu ! Donc $\underline{\alpha = 1}$.
• Dans le début de la question précédente, on n'avait pas utilisé le fait que $\alpha \neq 1$. La première relation reste donc valable, et, en remplaçant α par 1, elle s'écrit : $g\mathbf{o}f + \beta g = 0$ d'où $f\mathbf{o}g = \alpha f$ soit $\underline{f\mathbf{o}g = f}$.
• Il en découle immédiatement : $\underline{\text{Ker}g \subset \text{Ker}f}$.
• En composant l'égalité $g\mathbf{o}f = f\mathbf{o}g - \alpha f - \beta g$ par f à gauche, on obtient : $f\mathbf{o}g\mathbf{o}f = f^2\mathbf{o}g - \alpha f^2 - \beta f\mathbf{o}g$, d'où, compte tenu de $f\mathbf{o}g = f$ et de $f^2 = f$: $(\alpha+\beta)f = 0$ d'où $\underline{\alpha + \beta = 0}$.
• On a donc $f\mathbf{o}g - g\mathbf{o}f = f - g$, d'où $g\mathbf{o}f = g$ et on en déduit facilement $\text{Ker}f \subset \text{Ker}g$, puis $\underline{\text{Ker}f = \text{Ker}g}$.

ii) Soient f, g des projecteurs tels que $f\mathbf{o}g = f$ et $\text{Ker}f \subset \text{Ker}g$. Alors, si $x \in \text{Im}f$, $(g\mathbf{o}f)(x) = g[f(x)] = g(x)$ et si $x \in Ker f, (g\mathbf{o}f)(x) = g[f(x)] = 0 = g(x)$; donc $g\mathbf{o}f$ et g coïncident sur deux sous-espaces vectoriels supplémentaires donc sont égales ; ainsi, $g\mathbf{o}f = g$ d'où $\underline{\varphi_g(f) = f - g}$.

3°) Compte tenu de ce qui précède, il suffit de montrer que le cas $\alpha = 0$ est impossible.
Si on avait $\alpha = 0$, on aurait $f\mathbf{o}g - g\mathbf{o}f = \beta g$, d'où, en composant à gauche puis à droite par g : $g\mathbf{o}f\mathbf{o}g - g\mathbf{o}f = \beta g$ et $f\mathbf{o}g - g\mathbf{o}f\mathbf{o}g = \beta g$, d'où en additionnant $\beta g = f\mathbf{o}g - g\mathbf{o}f = 2\beta g$ d'où $\beta = 0$ puis $f\mathbf{o}g = g\mathbf{o}f$, ce qui est exclu...

PROBLÈME 2

Première partie :

1°) Si $\mathbb{K}$ est un sous-corps de $\mathbb{R}$, il contient 0 et 1. Étant stable par addition et soustraction, il contient $\mathbb{Z}$. Étant stable par division, il contient $\mathbb{Q}$.

2°) a) • $I(\alpha) \neq \emptyset$ puisque le polynôme nul appartient à $I(\alpha)$.
• Si P et Q appartiennent à $I(\alpha)$, il est immédiat que $P + Q$ aussi.
• Enfin, si $P \in I(\alpha)$ et $A \in \mathbb{K}[X]$, alors $(AP)(\alpha) = A(\alpha)P(\alpha) = 0$ donc $AP \in I(\alpha)$.

Cela prouve que $\underline{I(\alpha) \text{ est un idéal de } \mathbb{K}[X]}$.
De plus, cet idéal n'est pas réduit à $\{0\}$, car on a supposé α algébrique. D'après le cours ($\mathbb{K}[X]$ est principal), il s'agit de l'idéal engendré par un polynôme (non nul) normalisé et un seul, M_α.

b) Si on avait $M_\alpha = AB$, avec $A, B \in \mathbb{K}[X]$, alors $A(\alpha)B(\alpha) = 0$. Si par ex. $A(\alpha) = 0$, $A \in I(\alpha)$ donc M_α divise A et puisque l'on a aussi A divise M_α, on a $M_\alpha = \lambda A$ avec $\lambda \in \mathbb{Q}$, d'où $B = \lambda$.

c) Il suffit donc de montrer que, si P est normalisé et irréductible dans $\mathbb{K}[X]$ et $P(\alpha) = 0$, alors $P = M_\alpha$.
Si P est un tel polynôme on a $P \in I(\alpha)$ donc $P = QM_\alpha$. Or P est irréductible dans $\mathbb{K}[X]$

donc $Q \in \mathbb{K}$ ou $M_\alpha \in \mathbb{K}$. Mais $M_\alpha \notin \mathbb{K}$ car $M_\alpha(\alpha) = 0$ et que M_α n'est pas la constante nulle. Donc $Q = \lambda \in \mathbb{K}$ et, comme P et M_α sont normalisés, $\lambda = 1$ et $P = M_\alpha$.

3°) $(i) \Rightarrow (iii)$ $\alpha \in \mathbb{K}$ implique que, pour tout $p \in \mathbb{N}$ $\alpha^p \in \mathbb{K}$, donc $\mathbb{K}[\alpha] \subset \mathbb{K}$ et donc $\mathbb{K}[\alpha] = \mathbb{K}$ car $1 \in \mathbb{K}[\alpha] \Rightarrow \lambda = \lambda.1 \in \mathbb{K}[\alpha]$ pour tout $\lambda \in \mathbb{K}$.
$(iii) \Rightarrow (ii)$ $\alpha \in \mathbb{K}[\alpha] = \mathbb{K}$ donc α est racine de $P = X - \alpha \in \mathbb{K}[X]$ normalisé et irréductible et donc $M_\alpha = X - \alpha$ qui est de degré 1.
$(ii) \Rightarrow (i)$ $M_\alpha = X + c$ avec $c \in \mathbb{K}$ et donc $M_\alpha(\alpha) = 0$ donne $\alpha = -c \in \mathbb{K}$.
Les trois propositions sont bien équivalentes .

4°) **a)** On montre facilement par récurrence que $\forall p \geqslant 2,\ \alpha^p \in \text{Vect}(1, \alpha)$.
En effet : on a $M_\alpha = X^2 - sX + p$ et $M_\alpha(\alpha) = 0$ donc $\alpha^2 = s\alpha - p \in \text{Vect}(1, \alpha)$ et, si $\alpha^p = a_p\alpha + b_p$, $\alpha^{p+1} = a_p\alpha^2 + b_p\alpha \in \text{Vect}(1, \alpha)$ d'après ci-dessus.
On a donc $\mathbb{K}[\alpha] \subset \text{Vect}(1, \alpha)$ donc la dimension de $\mathbb{K}[\alpha]$ est inférieure à 2. Comme $\mathbb{K} \subset \mathbb{K}[\alpha]$, elle est supérieure à 1 et, si elle était égale à 1, on aurait $\mathbb{K}[\alpha] = \mathbb{K}$ et le degré de α serait 1 d'après la question précédente.
Donc $\dim(\mathbb{K}[\alpha]) = 2$ (et $(1, \alpha)$ en est une base).

b) $\mathbb{K}[\alpha]$ étant un sous-anneau de $\mathbb{R}$, pour montrer que c'est un sous-corps de $\mathbb{R}$, il suffit de montrer que, si $x \in \mathbb{K}[\alpha]$ est non nul, alors $1/x \in \mathbb{K}[\alpha]$.
Soit $M_\alpha = X^2 - sX + p$ et β l'autre racine de M_α. $\alpha + \beta = s$ prouve que $\beta \in \mathbb{K}[\alpha]$. Soit $x \in \mathbb{K}[\alpha]$, $x \neq 0$. x s'écrit $a + b\alpha$, avec $(a, b) \in \mathbb{K}^2 - \{(0, 0)\}$. On a alors $(a + b\alpha)(a + b\beta) = a^2 - sab + pb^2 \in \mathbb{K}$, et ce nombre est non nul puisque $(a + b\alpha)$ et $(a + b\beta)$ sont non nuls.
On a donc $\dfrac{1}{x} = \dfrac{a + b\beta}{a^2 - sab + pb^2} \in \mathbb{K}[\alpha]$.
Donc $\mathbb{K}[\alpha]$ est un corps .

c) Soit $k = s^2 - 4p$ le discriminant du trinôme M_α. k est positif ou nul (car ce trinôme a des racines !), et il ne peut pas être nul sinon α serait dans $\mathbb{K}$ et $\mathbb{K}[\alpha]$ serait de dimension 1. Donc $k > 0$. On a $\alpha = \dfrac{s \pm \sqrt{k}}{2}$ donc $\alpha \in \mathbb{K}[\sqrt{k}]$ donc $\mathbb{K}[\alpha] \subset \mathbb{K}[\sqrt{k}]$. On a aussi $\sqrt{k} = \pm(2\alpha - s) \in \mathbb{K}[\alpha]$ donc $\sqrt{k} \in K[\alpha]$ donc $\mathbb{K}[\sqrt{k}] \subset \mathbb{K}[\alpha]$, puis le résultat.

5°) **a)** •Tout $x \in \mathbb{K}[\alpha]$ s'écrit $x = P(\alpha)$ avec $P \in \mathbb{K}[X]$ et, par division euclidienne, $P = QM_\alpha + R$ avec $\deg(R) \leqslant n - 1$ donc $x = Q(\alpha)M_\alpha(\alpha) + R(\alpha) = R(\alpha)$. Cela démontre l'existence de R.
Pour l'unicité : si $x = R_1(\alpha) = R_2(\alpha)$ avec $\deg(R_i) \leqslant n - 1$ alors $R_1 - R_2 \in I(\alpha)$ donc M_α divise $R_1 - R_2$ et $\deg(R_1 - R_2) \leqslant n - 1$ ce qui donne $R_1 - R_2 = 0$.
• Soit $\psi : \begin{array}{ccc} \mathbb{K}_{n-1}[X] & \to & \mathbb{K}[\alpha] \\ R & \mapsto & R(\alpha) \end{array}$. ψ est linéaire et ce qui précède montre que ψ est bijective.
ψ est donc un isomorphisme et transforme une base de $\mathbb{K}_{n-1}[X]$ en une base de $\mathbb{K}[\alpha]$.
Donc $\dim(\mathbb{K}[\alpha]) = n$ et une base de $\mathbb{K}[\alpha]$ est $(1, \alpha, \ldots, \alpha^{n-1})$.

b) Le fait que φ est $\mathbb{K}$-linéaire et injective est immédiat. $\mathbb{K}[\alpha]$ étant un anneau, φ est donc un endomorphisme injectif du $\mathbb{K}$-espace vectoriel de dimension finie $\mathbb{K}[\alpha]$. Il est donc bijectif ; en particulier, il existe $y \in \mathbb{K}[\alpha]$ tel que $xy = 1$: tout élément non nul de $\mathbb{K}|\alpha]$ est donc inversible dans $\mathbb{K}[\alpha]$, et $\mathbb{K}[\alpha]$ est un corps .

c) On sait déjà que $\mathbb{K}[\alpha]$ est un corps contenant α et $\mathbb{K}$ et inclus dans $\mathbb{R}$.
Si $\mathbb{L}$ est un corps contenant α et $\mathbb{K}$ alors, par stabilité par $+$ et $\times$, il contient tous les $x = \sum_{p=0}^{q} x_p\alpha^p$ avec $q \in \mathbb{N}$ et $x_p \in \mathbb{K}$ et donc il contient $\mathbb{K}[\alpha]$.

Donc $\mathbb{K}[\alpha]$ est le plus petit sous-corps de $\mathbb{R}$ contenant α et $\mathbb{K}$.

6°) **a)** $\alpha = \sqrt{2}$ est racine de $X^2 - 2$; pour justifier que $X^2 - 2$ est bien le polynôme $\mathbb{Q}$-minimal de $\sqrt{2}$ il suffit de vérifier que $\sqrt{2}$ n'est racine d'aucun polynôme non nul de degré inférieur ou égal à 1 de $\mathbb{Q}[X]$, c'est à dire que $\sqrt{2}$ n'est pas dans $\mathbb{Q}$.
Le résultat est connu, mais je redonne la demonstration : on raisonne par l'absurde : si $\sqrt{2} = \dfrac{p}{q}$ avec $p, q \in \mathbb{Z} \setminus \{0\}$ premiers entre eux, on aurait $p^2 = 2q^2$ donc 2 divise p , soit $p = 2p'$; il vient $2p'^2 = q^2$ donc 2 divise q ; 2 est diviseur commun à p et q ce qui contredit l'hypothèse p, q premiers entre eux. Par conséquent, $\sqrt{2}$ n'est pas rationnel et
$X^2 - 2$ est le polynôme $\mathbb{Q}$-minimal de $\sqrt{2}$.

b) $\alpha = \sqrt[3]{2}$ est racine de $X^3 - 2$; pour justifier que $X^3 - 2$ est bien le polynôme $\mathbb{Q}$-minimal de $\sqrt[3]{2}$, il suffit de vérifier que ce polynôme est irréductible dans $\mathbb{Q}[X]$. Si on avait $X^3 - 2 = A.B$ avec A, B dans $\mathbb{Q}[X]$ non constants, l'un des deux polynômes A ou B serait de degré 1, et $\sqrt[3]{2}$ serait dans $\mathbb{Q}$, ce qui n'est pas (dém. semblable à la précédente).

c) Soit $\alpha = \sqrt{\dfrac{1+\sqrt{5}}{2}}$; on a $\alpha^2 = \dfrac{1+\sqrt{5}}{2}$ d'où $(2\alpha^2 - 1)^2 = 5$, ou encore $\alpha^4 - \alpha^2 - 1 = 0$.
Donc α est racine du polynôme $P = X^4 - X^2 - 1$: pour montrer que ce polynôme est le polynôme $\mathbb{Q}$-minimal de α, il suffit de montrer que P est irréductible dans $\mathbb{Q}[X]$.

Pour montrer que P n'a pas de diviseur dans $\mathbb{Q}[X]$ de degré 1, il suffit de vérifier que P n'a pas de racine rationnelle. Par l'absurde, si $\dfrac{p}{q} \neq 0$ (P n'admet pas 0 pour racine) était une telle racine ($p \in \mathbb{Z}$ et $q \in \mathbb{N} \setminus \{0\}$ avec p, q premiers entre eux), on aurait $p^4 - p^2q^2 - q^4 = 0$ donc $p^4 = (p^2 + q^2)q^2$ d'ou q divise p^4 ; or q est aussi premier avec p^4 , donc $q = 1$. Alors $p^4 - p^2 - 1 = 0$ entraîne que p divise 1 donc $p = \pm 1$. On constate immédiatement que 1 et -1 ne sont pas racines de P donc P n'a pas de diviseur de degré 1 et par suite n'a pas non plus de diviseur de degré 3.

Montrons maintenant que P n'a pas de diviseur de degré 2 dans $\mathbb{Q}[X]$. Sinon P serait produit de deux polynômes de degré 2 que l'on peut supposer normalisés :
$X^4 - X^2 - 1 = P = (X^2 + bX + c)(X^2 + b'X + c')$.
L'identification donne $b' + b = 0$, $c' + bb' + c = -1$, $bc' + cb' = 0$, $cc' = -1$. On a donc $b' = -b$; si $b \neq 0$, on a $c' = c$ et $c^2 = -1$ ce qui est impossible. Par suite $b = b' = 0$, $c' = -c - 1$ et $c^2 + c - 1 = 0$. On vérifie encore que cette dernière équation n'a pas de racine dans $\mathbb{Q}$: si $\dfrac{p}{q}$ irréductible est racine, $p^2 + pq - q^2 = 0$ donc q divise p^2 et est premier avec p^2 , d'où $q = 1$; puis $p^2 + p - 1 = 0$ donc p divise 1 et $p = \pm 1$; comme 1 et -1 ne sont pas racine de $X^2 + X - 1$ on a la contradiction cherchée. P n'a pas de diviseur de degré 2 dans $\mathbb{Q}[X]$.
Ainsi $P = X^4 - X^2 - 1$ est irréductible dans $\mathbb{Q}[X]$ et c'est le polynôme $\mathbb{Q}$-minimal de $\sqrt{\dfrac{1+\sqrt{5}}{2}}$.

7°) **a)** $Q_{n+2}(x) = P_{n+2}(\dfrac{x}{2}) = xQ_{n+1}(x) - Q_n(x)$. Cette relation permet de démontrer facilement par récurrence que Q_n est à coefficients entiers, normalisé, de degré n. On en déduit que P_n est de degré n et de coefficient dominant 2^n.
Par récurrence également, on montre que $P_{2n}(0) = P_{2n+1}(0) = (-1)^n$.
On calcule : $P_2 = 4X^2 + 2X - 1$, $\quad P_3 = 8X^3 + 4X^2 - 4X - 1$,
$P_4 = 16X^4 + 8X^3 - 12X^2 - 4X + 1$

b) • Même principe que dans la question **6°)** : si $\frac{p}{q} \neq 0$ (P_n n'admet pas 0 pour racine) est une racine de Q_n ($p \in \mathbb{Z}$ et $q \in \mathbb{N} \setminus \{0\}$ avec p, q premiers entre eux), on aurait, en posant $Q_n(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$ ($a_i \in \mathbb{Z}$), en multipliant par q^n : $p^n + \sum_{i=0}^{n-1} a_i p^i q^{n-i} = 0$ d'où $p\left(p^{n-1} + \sum_{i=1}^{n-1} a_i p^{i-1} q^{n-i}\right) = -a_0 q^n$ et $p^n = q\left(-\sum_{i=0}^{n-1} a_i p^i q^{n-i-1}\right)$. Donc q divise p^n ; étant premier avec p, on a $q = 1$. Puis p divise $a_0 q^n = \pm 1$, d'où $p = \pm 1$.
Ainsi, les seules racines rationnelles possibles de Q_n sont -1 et 1 .
• $Q_{n+3}(x) + xQ_n(x) = xQ_{n+2}(x) - Q_{n+1}(x) + xQ_n(x) = x^2 Q_{n+1}(x) - xQ_n(x) - Q_{n+1}(x) + xQ_n(x) = (x^2-1)Q_{n+1}(x)$ soit $\underline{Q_{n+3}(x) + xQ_n(x) = (x^2-1)Q_{n+1}(x)}$.
• Pour $x = \pm 1$, on a $Q_{n+3}(x) = \pm Q_n(x)$ d'où le résultat (car les seules racines rationnelles possibles de Q_n sont -1 et 1).
• Q_0 n'a pas de racine rationnelle, Q_1 a pour seule racine rationnelle 1 et $Q_2 = X^2 + X - 1$ n'a pas de racine rationnelle. Donc Q_{3k} et Q_{3k+2} n'ont pas de racine rationnelle et Q_{3k+1} a pour seule racine rationnelle -1. Donc :
$\underline{P_{3k} \text{ et } P_{3k+2} \text{ n'ont pas de racine rationnelle et } P_{3k+1} \text{ a pour seule racine rationnelle } -\frac{1}{2}}$.

8°) **a)** L'équation caractéristique de la récurrence est $X^2 - 2\cos\theta X + 1 = 0$ qui a pour discriminant réduit $-\sin^2\theta \neq 0$ et pour solutions (dans $\mathbb{C}$) $e^{i\theta}$ et $e^{-i\theta}$. Il existe donc $(\lambda, \mu) \in \mathbb{R}^2$ tels que $\forall n,\ u_n = \lambda\cos(n\theta) + \mu\sin(n\theta)$. En particulier $u_0 = \lambda$ et $u_1 = \lambda\cos\theta + \mu\sin\theta$ d'où $\underline{\forall n,\ u_n = u_0\cos(n\theta) + \frac{u_1 - u_0\cos\theta}{\sin\theta}\sin(n\theta)}$.

b) • $v_n = P_n(\cos\theta)$ vérifie $v_{n+2} = 2\cos\theta v_{n+1} - v_n$, $v_0 = 1, v_1 = 2\cos\theta + 1$ donc

$$\begin{aligned} v_n &= \cos(n\theta) + \frac{2\cos\theta + 1 - \cos\theta}{\sin\theta}\sin(n\theta) \\ &= \cos(n\theta) + \frac{\cos\theta + 1}{\sin\theta}\sin(n\theta) \\ &= \cos(n\theta) + \frac{2\cos^2\left(\frac{\theta}{2}\right)}{2\cos\left(\frac{\theta}{2}\right)\sin\left(\frac{\theta}{2}\right)}\sin(n\theta) \\ &= \frac{\cos(n\theta)\sin\left(\frac{\theta}{2}\right) + \sin(n\theta)\cos\left(\frac{\theta}{2}\right)}{\sin\left(\frac{\theta}{2}\right)} \end{aligned}$$

Donc $\underline{\forall n,\ v_n = \frac{\sin\left((n+\frac{1}{2})\theta\right)}{\sin\left(\frac{\theta}{2}\right)}}$.

• On a $\forall k \in [\![1, n]\!],\ \frac{2k\pi}{2n+1} \in]0, \pi[$ donc, d'une part, d'après ce qui précède,
$\forall k \in [\![1, n]\!],\ P_n\big(\cos(\frac{2k\pi}{2n+1})\big) = \frac{\sin(k\pi)}{\sin\big(\frac{2k\pi}{2n+1}\big)} = 0$ et, d'autre part, les $\cos(\frac{2k\pi}{2n+1})$ sont deux à deux distincts. Comme P_n est de degré n, il ne peut avoir plus de n racines distinctes et donc on a exactement les racines de P_n.
$\underline{\text{Les racines de } P_n \text{ sont les } x_{k,n} = \cos(\frac{2k\pi}{2n+1}) \text{ pour } k \in [\![1, n]\!]}$.

c) • $\cos(\frac{2\pi}{5})$,$\cos(\frac{2\pi}{7})$ et $\cos(\frac{2\pi}{9})$ sont respectivement racines de P_2, P_3 et P_4 qui ont des coefficients entiers donc sont algébriques sur $\mathbb{Q}$.

• $\cos(\frac{2\pi}{5})$ est racine de $\frac{1}{4}P_2$ qui appartient à $\mathbb{Q}[X]$, est normalisé et irréductible dans $\mathbb{Q}[X]$ car sinon il aurait deux racines rationnelles ($\deg P_2 = 2$) or P_2 n'a pas de racine rationnelle.
Donc $M_{\cos(\frac{2\pi}{5})} = \frac{1}{4}P_2 = X^2 + \frac{1}{2}X - \frac{1}{4}$.

• $\cos(\frac{2\pi}{7})$ est racine de $\frac{1}{8}P_3$ qui appartient à $\mathbb{Q}[X]$ et est normalisé. Si il n'était pas irréductible dans $\mathbb{Q}[X]$, comme son degré est 3, il aurait au moins un facteur de degré 1 donc une racine rationnelle, or P_3 n'a pas de racine rationnelle.
Donc $M_{\cos(\frac{2\pi}{7})} = \frac{1}{8}P_3 = X^3 + \frac{1}{2}X^2 - \frac{1}{2}X - \frac{1}{8}$.

• $\cos(\frac{2\pi}{9}) \neq -\frac{1}{2}$ et $-\frac{1}{2}$ est racine (simple) de P_4 donc $\cos(\frac{2\pi}{9})$ est racine de $\frac{P_4}{16(X+\frac{1}{2})} = X^3 - \frac{3}{4}X + \frac{1}{8}$. Ce polynôme n'a pas de racine rationnelle donc est irréductible dans $\mathbb{Q}[X]$ (comme pour P_3 ci-dessus), il est normalisé donc $M_{\cos(\frac{2\pi}{9})} = \frac{P_4}{16(X+\frac{1}{2})} = X^3 - \frac{3}{4}X + \frac{1}{8}$.

9°) **a)** • M_α est de degré 3 donc, d'après **I-4°)**, $\dim(\mathbb{Q}[\alpha]) = 3$ et une de ses bases est $\mathcal{B} = (1, \alpha, \alpha^2)$.
• $\cos(\frac{4\pi}{9}) = \cos(2\frac{2\pi}{9})$ soit $\cos(\frac{4\pi}{9}) = 2\alpha^2 - 1$ et $\cos(\frac{2\pi}{9}) + \cos(\frac{4\pi}{9}) + \cos(\frac{8\pi}{9}) = 0$ (somme des racines de M_α) donc $\cos(\frac{8\pi}{9}) = -2\alpha^2 - \alpha + 1$.

b) • Soit $a \in \mathbb{Q}[\alpha]$ tel que $f(a) \neq 0$ (un tel a existe car on a supposé $f \neq 0$) ; on a $f(a) = f(a.1) = f(a)f(1)$ donc $f(1) = 1$.
D'autre part, $0 = f(0) = f\left(\alpha^3 - \frac{3}{4}\alpha + \frac{1}{8}\right) = (f(\alpha))^3 - \frac{3}{4}f(\alpha) + \frac{1}{8}$ donc $f(\alpha)$ est une racine de M_α c'est à dire $f(\alpha) \in \left\{\cos(\frac{2\pi}{9}), \cos(\frac{4\pi}{9}), \cos(\frac{8\pi}{9})\right\}$.
Comme $f(\alpha^2) = (f(\alpha))^2$ et que f est déterminée par l'image de la base $\mathcal{B}$, on obtient ainsi trois applications *possibles* définies par $f_k(\alpha) = \cos(\frac{2k\pi}{9})$ avec $k = 1, 2, 3$.

Réciproquement, soit β une des trois racines de M_α, et f définie sur $\mathbb{Q}[\alpha]$ par :
$\forall (x, y, z) \in \mathbb{Q}^3,\ f(x + y\alpha + z\alpha^2) = x + y\beta + z\beta^2$. Il faut alors vérifier que f est bien un endomorphisme du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[\alpha]$ (ça, c'est facile), et aussi de l'anneau $\mathbb{Q}[\alpha]$ (là, il y a un peu plus de calcul, que je vous laisse le soin de faire ; utiliser le fait que α et β sont racines de M_α pour exprimer α^3 et α^4 en fonction de $1, \alpha, \alpha^2$ et β^3 et β^4 en fonction de $1, \beta, \beta^2$...).

• $\mathbb{Q}[\beta] \subset \mathbb{Q}[\alpha]$ mais $\dim(\mathbb{Q}[\beta]) = 3$ (car le polynôme minimal de β est M_α), et donc $\mathbb{Q}[\beta] = \mathbb{Q}[\alpha]$, ce qui nous permet de conclure que $(1, \beta, \beta^2)$ est une base de $\mathbb{Q}[\alpha]$.
Soit $f \in \{f_1, f_2, f_3\}$; f transforme la base $\mathcal{B}$ en une base de $\mathbb{Q}[\alpha]$ donc f est bijective donc $\{f_1, f_2, f_3\} \subset \mathrm{GL}(\mathbb{Q}[\alpha])$.
Soit $(f, g) \in \{f_1, f_2, f_3\}^2$, $g\mathbf{o}f^{-1} \in \mathcal{L}(\mathbb{Q}[\alpha])$ et
$g\mathbf{o}f^{-1}(xy) = g\mathbf{o}f^{-1}\left(f\left(f^{-1}(x)\right) f\left(f^{-1}(y)\right)\right) = g\mathbf{o}f^{-1}\left(f\left(f^{-1}(x)f^{-1}(y)\right)\right) = gleft(f^{-1}(x)f^{-1}(y)) = g\mathbf{o}f^{-1}(x)g\mathbf{o}f^{-1}(x)$. Donc $g\mathbf{o}f^{-1} \in \{f_1, f_2, f_3\}$.
Donc $\{f_1, f_2, f_3\}$ est un groupe (sous-groupe de $\mathrm{GL}(\mathbb{Q}[\alpha])$.

• $f_1 = \mathrm{Id}_{\mathbb{Q}[\alpha]}$.
$f_2(\alpha) = 2\alpha^2 - 1$ donc $f_2(\alpha^2) = 4\alpha^4 - 4\alpha^2 + 1 = 4\alpha\left(\alpha^3 - \frac{3}{4}\alpha + \frac{1}{8}\right) - \alpha^2 - \frac{1}{2}\alpha + 1 =$

$-\alpha^2 - \frac{1}{2}\alpha + 1$.
$f_3(\alpha) = -2\alpha^2 - \alpha + 1$ donc $f_3(\alpha^2) = (2\alpha^2-1)^2 + 2\alpha((2\alpha^2-1) + \alpha^2 = -\alpha^2 - \frac{1}{2}\alpha + 1 + 4\left(\alpha^3 - \frac{3}{4}\alpha + \frac{1}{8}\right) + \alpha - \frac{1}{2} + \alpha^2 = \frac{1}{2}\alpha + \frac{1}{2}$.
Les matrices dans $\mathcal{B}$ sont donc :

$$M(f_1,\mathcal{B}) = I_3, \qquad M(f_2,\mathcal{B}) = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 0 & -\frac{1}{2} \\ 0 & 2 & -1 \end{pmatrix}, \qquad M(f_3,\mathcal{B}) = \begin{pmatrix} 1 & 1 & \frac{1}{2} \\ 0 & -1 & \frac{1}{2} \\ 0 & -2 & 0 \end{pmatrix}$$

10°) **a)** Soit C_S un dénominateur (positif) commun aux coefficients de S ; S s'écrit alors $S(x) = \dfrac{1}{C_S}\sum_{i=0}^{n} a_i x^i$ avec $a_i \in \mathbb{Z}$.

On a donc $S(r) = \dfrac{1}{C_S q^n}\sum_{i=0}^{n} a_i p^i q^{n-i}$. Or $\sum_{i=0}^{n} a_i p^i q^{n-i} \in \mathbb{Z}$ et est non nul car sinon $r \in \mathbb{Q}$ serait racine de S qui ne serait pas irréductible dans $\mathbb{Q}[X]$. On a donc $\left|\sum_{i=0}^{n} a_i p^i q^{n-i}\right| \geqslant 1$ et donc $\underline{|S(r)| \geqslant \dfrac{1}{C_S q^n}}$.

b) Soit $M = \sup_{t\in[\alpha-1,\alpha+1]} |S'(t)|$. L'inégalité des accroissements finis s'écrit, pour tout $r \in [\alpha-1, \alpha+1]$, $|S(r)| = |S(r) - S(\alpha)| \leqslant M|\alpha - r|$ et, pour $r \in \mathbb{Q}$ en particulier, on obtient $\dfrac{1}{C_S q^n} \leqslant M|\alpha - r|$.
Donc, en posant $K = \dfrac{1}{MC_S} > 0$,
$\underline{\exists K > 0,\ \forall r = \dfrac{p}{q} \in \mathbb{Q} \cap [\alpha-1, \alpha+1],\ (q>0) \quad |\alpha - r| \geqslant \dfrac{K}{q^n}}$.

c) • Version 5/2 : $\forall k \geqslant 1,\ 10^{-k!} \leqslant 10^{-k}$ et $\left(\sum 10^{-k}\right)$ converge donc $\underline{(t_n) \text{ converge}}$ et , de plus, $\forall n,\ t - t_n = \sum_{k=n+1}^{+\infty} 10^{-k!} = 10^{-(n+1)!}\sum_{k=n+1}^{+\infty} 10^{(n+1)!-k!} = 10^{-(n+1)!}\sum_{k=n+1}^{+\infty} 10^{(n+1)!-k!}$. Or, pour $k \geqslant n+2$, $k! - (n+1)! = (n+1)!\left(\prod_{i=n+2}^{k} i - 1\right) \geqslant (n+1)!(k-1) \geqslant k-1 \geqslant k-n-1$,
inégalité vraie aussi pour $k = n+1$, et donc $0 \leqslant t - t_n \leqslant 10^{-(n+1)!}\sum_{k=n+1}^{+\infty} 10^{-(k-n-1)} = 10^{-(n+1)!}\dfrac{1}{1-10^{-1}} = \dfrac{10}{9}10^{-(n+1)!}$. Donc $\underline{|t - t_n| \leqslant 2.10^{-(n+1)!}}$.

• Version 3/2 : (t_n) est croissante et $\forall n,\ t_n \leqslant 10^{-1} + \sum_{k=1}^{n} 10^{-k} \leqslant 1 + \sum_{k=1}^{n} 10^{-k} = \dfrac{1-10^{-(n+1)}}{1-10^{-1}} \leqslant \dfrac{10}{9}$ et donc $\underline{(t_n) \text{ converge}}$. Et, comme ci-dessus, on a $t_{n+p} - t_n \leqslant 10^{-(n+1)!}\sum_{k=n+1}^{n+p} 10^{-(k-n-1)} \leqslant \dfrac{10}{9}10^{-(n+1)!}$ et donc $\underline{|t - t_n| \leqslant 2.10^{-(n+1)!}}$.

• Supposons t algébrique de degré $d \geqslant 1$. En appliquant les résultats de **b)** à $S = M_t$, on a $\exists K > 0,\ \forall r = \dfrac{p}{q} \in \mathbb{Q} \cap [t-1, t+1],\ |t - r| \geqslant \dfrac{K}{q^d}$. Or, par définition de la limite, $\exists N,\ \forall n \geqslant N,\ t_n \in [t-1, t+1]$; d'autre part, $t_n = \dfrac{p}{10^{n!}}$ avec $p \in \mathbb{N}$ donc

$\forall n \geqslant N,\ |t - t_n| \geqslant \dfrac{K}{10^{dn!}}$. Ce qui précède donne $\forall n \geqslant N,\ 2.10^{-(n+1)!} \geqslant \dfrac{K}{10^{dn!}}$ soit $10^{-(n+1-d)n!} \geqslant \dfrac{K}{2}$. Mais $\lim\limits_{n\to+\infty} 10^{-(n+1-d)n!} = 0$ ce qui conduit à une contradiction.
t est transcendant sur $\mathbb{Q}$.

Seconde partie :

1°) • Soient $A\begin{pmatrix} a \\ b \end{pmatrix}$, $A'\begin{pmatrix} a' \\ b' \end{pmatrix}$ et $A''\begin{pmatrix} a'' \\ b'' \end{pmatrix}$ appartenant à $\mathcal{K}$.
La droite (AA') admet pour équation $(x-a)(b'-b) = (y-b)(a'-a)$ dont les coefficients sont dans $\mathbb{K}$ (somme et produit d'éléments de $\mathbb{K}$).
Le cercle de centre A et de rayon $A'A''$ a pour équation $(x-a)^2+(y-b)^2 = (a'-a'')^2+(b'-b'')^2$ dont les coefficients sont dans $\mathbb{K}$.
Toute droite de $\mathcal{D}$ et tout cercle de $\mathcal{C}$ ont une équation à coefficients dans $\mathbb{K}$.
• $(\Delta, \Delta') \in \mathcal{D}^2$ d'équations à coefficients dans $\mathbb{K}$, $ax+by = c$ et $a'x+b'y = c'$, non parallèles, ont pour point commun $M\begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$ dont les coordonnées sont données par les formules de Cramer $x_0 = \dfrac{cb'-c'b}{ab'-a'b} \in \mathbb{K}$, et $y_0 = \frac{ac'-a'c}{ab'-a'b} \in \mathbb{K}$.
Le point commun de deux droites sécantes de $\mathcal{D}$ appartient à $\mathcal{K}$.
• Soit $\Delta = (AA') \in \mathcal{D}$ avec $(A, A') \in \mathcal{K}^2$, on peut la paramétrer par $\begin{cases} x = a + t(a'-a) \\ y = b + t(b'-b) \end{cases}$ avec $t \in \mathbb{R}$. Soit $\Gamma \in \mathcal{C}$ d'équation à coefficients dans $\mathbb{K}$ $x^2+y^2-2\alpha x-2\beta y+\gamma = 0$. Le paramètre t_0 d'un des points $M(t_0)$ communs à Δ et Γ (si il en existe) est donc donné par une équation de degré inférieur ou égal à 2 à coefficients dans $\mathbb{K}$. Donc t_0 est algébrique de degré 1 ou 2. Si son degré est 1, $t_0 \in \mathbb{K}$ et les coordonnées de $M(t_0)$ aussi. Si son degré est 2, les coordonnées de $M(t_0)$ appartiennent à $\mathbb{K}[t_0]$ qui est alors une extension quadratique de $\mathbb{K}$.
• Soient $(\Gamma, \Gamma') \in \mathcal{C}^2$ deux cercles d'équations à coefficients dans $\mathbb{K}$ $x^2+y^2-2\alpha x-2\beta y+\gamma = 0$ et $x^2+y^2-2\alpha' x-2\beta' y+\gamma' = 0$. Les points communs à Γ et Γ' sont donnés par :

$$\begin{cases} x^2+y^2-2\alpha x-2\beta y+\gamma = 0 \\ x^2+y^2-2\alpha' x-2\beta' y+\gamma' = 0 \end{cases} \iff \begin{cases} x^2+y^2-2\alpha x-2\beta y+\gamma = 0 \\ 2(\alpha'-\alpha)x+2(\beta'-\beta)y = \gamma'-\gamma \end{cases}$$

On est donc ramené au cas précédent (intersection droite-cercle).

2°) **a)** • On trace les cercles de centre A et rayon AB et de centre C et rayon CB. Ils se coupent en B et D avec $AD = AB$ et $CD = CB$ c'est-à-dire tel que $ABCD$ parallélogramme.
Donc D est constructible à partir de $\{A, B, C\}$.
• Il suffit de choisir deux points B, C de Δ puis de construire D comme ci-dessus et la droite cherchée est (AD).
La parallèle à Δ passant par A est constructible à partir de $\{A, \Delta\}$.

b) **i)** J est l'intersection de (OI) avec le cercle de centre O et de rayon OI ; la droite (Oy) est la droite (MM') où M et M' sont les points communs des cercles de centres respectifs I et J et de rayon (par exemple) IJ ; le point K est l'intersection de (Oy) avec le cercle de centre O et de rayon OI. Donc J et K sont constructibles .

ii) • Soient $A\begin{pmatrix} \alpha \\ 0 \end{pmatrix}$ $B\begin{pmatrix} \beta \\ 0 \end{pmatrix}$. Le cercle de centre B et rayon $|\alpha| = OA$ coupe (Ox) en $C\begin{pmatrix} \beta+|\alpha| \\ 0 \end{pmatrix}$ et $C'\begin{pmatrix} \beta-|\alpha| \\ 0 \end{pmatrix}$. Donc $\alpha+\beta$ est constructible .

• Traçons la parallèle à (KB) passant par A, elle coupe (Oy) en D tel que, d'après le théorème de Thalès, $\dfrac{OD}{OK} = \dfrac{OA}{OB}$ soit $OD = \dfrac{\alpha}{\beta}$. Donc $\dfrac{\alpha}{\beta}$ est constructible .

• Soit $A'\begin{pmatrix} 0 \\ \alpha \end{pmatrix}$ qui est constructible. On trace la parallèle à (KB) passant par A', elle coupe (Ox) en E tel que, d'après le théorème de Thalès , $\dfrac{OA'}{OK} = \dfrac{OE}{OB}$ soit $\alpha = \dfrac{OE}{\beta}$ et donc $OE = \alpha.\beta$. Donc $\alpha.\beta$ est constructible .

iii) *Lemilieu*A'*de*$[JA]$ est constructible car c'est l'intersection de (Ox) avec la médiatrice de $[JA]$ qu'on construit comme la droite (NN') avec N et N' les points communs des cercles de centres respectifs A et J et de rayon AJ. Le cercle de centre A' et de rayon AA' a pour équation $\left(x - \dfrac{\alpha-1}{2}\right)^2 + y^2 = \left(\dfrac{\alpha+1}{2}\right)^2$ et coupe donc (Oy) en $\begin{pmatrix} 0 \\ \pm\sqrt{\alpha} \end{pmatrix}$ (car $\left(\dfrac{\alpha+1}{2}\right)^2 - \left(\dfrac{\alpha-1}{2}\right)^2 = \alpha$). Donc $\sqrt{\alpha}$ est constructible.

3°) **a)** Soit M un point constructible ; il existe donc une suite finie de points M_1, M_2, …, $M_n = M$ telle que :
• M_1 soit construit à partir de l'ensemble des deux points O et I
• M_i pour $2 \leqslant i \leqslant n$, soit construit à partir de l'ensemble $\{O, I, M_1, M_2, \ldots, M_{i-1}\}$.
On posera $M_0 = I$ et $M_{-1} = O$. On démontre alors par récurrence sur $p \in [\![0, n]\!]$ qu'il existe une suite finie $(\mathbb{K}_i)_{0\leqslant i\leqslant q}$ de sous-corps du corps des réels $\mathbb{R}$ ayant la propriété (P) telle que les coordonnées des M_i pour $-1 \leqslant i \leqslant p$ appartiennent au corps $\mathbb{K}_q$.

◇ Cela est vrai pour $p = 0$, avec $q = 0$ et $\mathbb{K}_0 = \mathbb{Q}$, car les coordonnées de M_{-1} et M_0 sont rationnelles.

◇Si cela est vérifié à l'ordre $p \leqslant n-1$, soit alors une suite finie $(\mathbb{K}_i)_{0\leqslant i\leqslant q}$ de sous-corps du corps des réels $\mathbb{R}$ ayant la propriété (P) telle que les coordonnées des M_i pour $-1 \leqslant i \leqslant p$ appartiennent au corps $\mathbb{K}_q$.
On applique alors les résultats de la question précédente avec $\mathbb{K} = \mathbb{K}_q$: puisque les coordonnées de $M_{-1}, M_0, \ldots, M_p$ sont dans $\mathbb{K}_q$, les coordonnées de M_{p+1} sont, soit dans $\mathbb{K}_q$, auquel cas la suite $(\mathbb{K}_i)_{0\leqslant i\leqslant q}$ convient, soit dans une extension quadratique de $\mathbb{K}_p$ que l'on note $\mathbb{K}_{q+1}$. Dans ce dernier cas, la suite $(\mathbb{K}_i)_{0\leqslant i\leqslant q+1}$ vérifie la propriété (P) et les coordonnées des M_i pour $-1 \leqslant i \leqslant p+1$ sont toutes dans $\mathbb{K}_{q+1}$ puisque $\mathbb{K}_q \subset \mathbb{K}_{q+1}$.
Cela achève la récurrence et répond à la question.

b) Soit une suite finie $(\mathbb{K}_i)_{0\leqslant i\leqslant n}$ ayant la propriété (P) ; on montre par récurrence sur n que tous les points M du plan dont les coordonnées appartiennent au corps $\mathbb{K}_n$ sont constructibles.
◇ Pour $n = 0$, $\mathbb{K}_0 = \mathbb{Q}$, et les points à coordonnées rationnelles sont constructibles, car ceux à coordonnées entières le sont et on utilise la propriété : α, β constructibles $\Rightarrow \alpha/\beta$ constructible.
◇ Supposons que les éléments de $\mathbb{K}_n$ soient tous constructibles. Ceux de $\mathbb{K}_{n+1} = \mathbb{K}_n[\sqrt{k_n}]$ peuvent s'écrire sous la forme $x + y\sqrt{k_n}$, x, y, k_n étant dans $\mathbb{K}_n$. On construit $\sqrt{k_n}$ comme indiqué au II.2.b, puis le produit $y\sqrt{k_n}$ de même, enfin la somme suivant le procédé vu dans cette même question. En conséquence, tout élément de $\mathbb{K}_{n+1}$ est constructible.

4°) **a)** F est un sous-corps de H donc H est un F-espace vectoriel .
Soient $(g_1, \ldots, g_q)$ une base de G comme F-ev et $(h_1, \ldots, h_r)$ une base de H comme G-ev, montrons que $(g_1h_1, \ldots, g_qh_1, g_1h_2, \ldots, g_qh_r)$ est une base de H comme F-ev.

Soit $x \in H$, x s'écrit $x = \sum_{i=1}^{r} x_i h_i$ avec pour toout i, $x_i \in G$. Les x_i s'écrivent $x_i = \sum_{j=1}^{q} y_{i,j} g_j$ avec $y_{i,j} \in F$. On a donc $x = \sum_{i=1}^{r}\sum_{j=1}^{q} y_{i,j} g_j h_i$ donc la famille ci-dessus est génératrice du F-ev H.

D'autre part, si $\sum_{i=1}^{r}\sum_{j=1}^{q} y_{i,j} g_j h_i = 0$, soit $\sum_{i=1}^{r}\left(\sum_{j=1}^{q} y_{i,j} g_j\right) h_i = 0$ on a $\forall i,\ \sum_{j=1}^{q} y_{i,j} g_j$ donc $\forall i,\ \forall j,\ y_{i,j} = 0$ et la famille est aussi libre donc c'est une base de H et $\underline{\dim_F(H) = qr}$.

b) D'après **a.**, puisque, pour tout i, $\dim_{\mathbb{K}_{i-1}}(\mathbb{K}_i) = 2$, par une récurrence facile, on a $\underline{\dim_{\mathbb{Q}}(\mathbb{K}_n) = 2^n}$.

c) Si α est constructible, c'est-à-dire si $A(\alpha, 0)$ est constructible, il existe une suite $\mathbb{K}_0, \ldots, \mathbb{K}_n$ ayant la propriété (P) et telle que $\alpha \in \mathbb{K}_n$. Comme $\mathbb{K}_n$ est de dimension finie sur $\mathbb{Q}$, la famille $(\alpha^k)_{k\in\mathbb{N}}$ est liée sur $\mathbb{Q}$, autrement dit il existe $(\lambda_0, \ldots, \lambda_d) \neq (0, \ldots, 0)$ tels que $\sum_{k=0}^{d} \lambda_k \alpha^k = 0$ et donc α est algébrique sur $\mathbb{Q}$. On peut donc écrire, d'après **I-4°) d.**, $\mathbb{Q} \subset \mathbb{Q}[\alpha] \subset \mathbb{K}_n$. $\mathbb{K}_n$ est de dimension finie sur $\mathbb{Q}$ donc sur $\mathbb{Q}[\alpha]$ (une famille génératrice sur $\mathbb{Q}$ l'est a fortiori sur $\mathbb{Q}[\alpha]$) et on peut appliquer **a.** : $\dim_{\mathbb{Q}}(\mathbb{K}_n) = \dim_{\mathbb{Q}}(\mathbb{Q}[\alpha]) \dim_{\mathbb{Q}[\alpha]}(\mathbb{K}_n) = d(\alpha, \mathbb{Q}) \dim_{\mathbb{Q}[\alpha]}(\mathbb{K}_n)$ donc $d(\alpha, \mathbb{Q}) \mid \dim_{\mathbb{Q}}(\mathbb{K}_n) = 2^n$ et donc $\underline{\exists p \in \mathbb{N},\ d(\alpha, \mathbb{Q}) = 2^p}$.

d) • Soit Π_n le polygone régulier à n comme dans l'énoncé ; on a d'abord le résultat suivant :

$$\Pi_n \text{ constructible } \iff \cos\left(\frac{2\pi}{n}\right) \text{ constructible.}$$

En effet, si Π_n est constructible, A_2 est constructible et la parallèle à (Oy) passant par A_2 coupe (Ox) en $(\cos\left(\frac{2\pi}{n}\right), 0)$.

Réciproquement, si $\cos\left(\frac{2\pi}{n}\right)$ est constuctible, $(\cos\left(\frac{2\pi}{n}\right), 0)$ l'est et la parallèle à (Oy) passant par ce point coupe le cercle de centre O et rayon 1 en deux points A_2 et A_n. Il suffit ensuite de construire A_{i+1} à partir de A_i comme intersection du cercle de centre O et rayon 1 avec le cercle de centre A_i et de rayon A_1A_2.

• D'autre part, on a : Π_n constructible $\implies \Pi_{2n}$ constructible . En effet, la médiatrice de $[A_1A_2]$ est constructible (cf **II-2°) b.**) donc le point A_2' intersection du cercle de centre O et rayon 1 avec cette droite et d'ordonnée de même signe que celle de A_2 est constructible, et on construit Π_{2n} à partir de I et A_2' comme ci-dessus.

• $\cos\left(\frac{2\pi}{3}\right) = -\frac{1}{2} \in \mathbb{Q}$ donc est constructible et donc Π_3 et Π_6 sont constructibles.

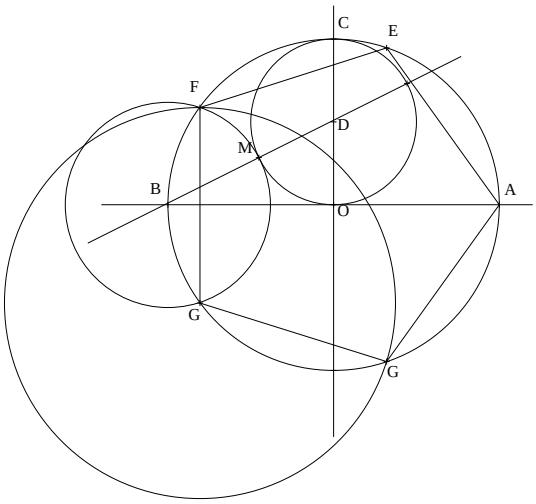
$\cos\left(\frac{2\pi}{4}\right) = 0$ est constructible donc Π_4 et Π_8 sont constructibles.

$\cos\left(\frac{2\pi}{5}\right) \in \mathbb{K}_1$ extension quadratique de $\mathbb{Q}$ d'après **I-6°) c.** donc il est constructible d'après **II-3°) b.** ce qui donne Π_5 et Π_{10} constructibles.

Enfin, d'après **I-6°) c.**, $\cos\left(\frac{2\pi}{7}\right)$ et $\cos\left(\frac{2\pi}{9}\right)$ ont pour degré 3sur $\mathbb{Q}$, donc ne sont pas constructibles d'après **II-4°) c.**.

Les polygones Π_n avec $n \in [\![3, 10]\!]$ sont constructibles à l'exception de Π_7 et Π_9 .

Construction du pentagone à la règle et au compas :



Notes historiques :

1) Ces problèmes de construction "à la règle et au compas" datent des Grecs, pour qui les seules courbes parfaites sont la droite et le cercle. [Ce genre d'a priori a d'ailleurs fortement marqué l'histoire de la pensée occidentale : c'est le principe que les seuls mouvements parfaits sont circulaires uniformes qui sous-tend le système astronomique de Ptolémée qui a régné comme modèle de l'univers jusqu'à Kepler et Gallilée.]
En mathématiques, trois problèmes sont restés célèbres : la duplication du cube (construire un cube de volume double) qui équivaut à $\sqrt[3]{2}$ constructible et qui est donc impossible ; la trisection de l'angle (couper en angle en 3 angles égaux) qui est, en général, impossible (voir le sujet de ENS P' 1978) ; et la célébrissime quadrature du cercle (construire un carré de même aire qu'un disque donné) qui équivaut à $\sqrt{\pi}$ constructible et qui est impossible car π est transcendant ce qui fut démontré par Lindemann en 1882.
Faute de trouver des solutions explicites et de pouvoir démontrer les impossibilités qu'on a vues au II (deux millénaires plus tard !), ils ont imaginé de faire appel à des courbes nouvelles, comme la Cissoïde de Dioclès ou la Conchoïde de Nicomède. Ces courbes leur permirent de réaliser la "trisection" de l'angle, donc de "construire" l'ennéagone , ou de "dupliquer le cube"

2) Gauss a démontré que pour qu'un polygone régulier à n côtés soit constructible, il suffit que, dans la décomposition de n en facteurs premiers, les termes de la forme p^r, avec p premier $\geqslant 3$, soient tels que p soit un nombre de Fermat ($2^{2^m}+1$) et que r soit égal à 1 . Il existe une construction (compliquée, due à Erchinger) du polygone à 17 côtés. On a en effet :

$$\cos\left(\frac{\pi}{17}\right) = \frac{1}{16}\left[1-\sqrt{17}+\sqrt{34-2\sqrt{17}}+\sqrt{68+12\sqrt{17}}+16\sqrt{34+2\sqrt{17}}-2(\sqrt{17}-1)\sqrt{34-2\sqrt{17}}\right]$$

formule qui prouve que ce nombre est constructible d'après II.2

* * *
* *
*