SESSION 1996

Concours commun Mines-Ponts

DEUXIEME EPREUVE. FILIERE M

Première partie

I-1) $I(\alpha)$ **est un idéal de** $\mathbb{K}[X]$
a) Soient $\alpha \in \mathbb{K}$ et $I(\alpha) = \{P \in \mathbb{K}[X] / \ P(\alpha) = 0\}$.
• $I(\alpha)$ contient le polynôme nul. De plus, si P et Q sont dans $I(\alpha)$ alors $(P-Q)(\alpha) = 0$ et $P-Q$ est dans $I(\alpha)$. Donc $I(\alpha)$ est un sous groupe de $(\mathbb{K}[X], +)$.
• Enfin, si P est dans $I(\alpha)$ et Q est dans $\mathbb{K}[X]$ alors $PQ(\alpha) = P(\alpha)Q(\alpha) = 0 \times Q(\times) = 0$ et PQ est dans $I(\alpha)$.
Finalement

$I(\alpha)$ est un idéal de $(\mathbb{K}[X], +, \times)$.

Existence de M_α**.** On sait que $(\mathbb{K}[X], +, \times)$ est un anneau principal et donc $I(\alpha)$ est un idéal principal, non réduit à $\{0\}$ par définition d'un nombre algébrique. Par suite, il existe un polynôme M non nul tel que $I(\alpha) = M\mathbb{K}[X]$. Si on pose $M_\alpha = \dfrac{M}{\text{dom}(M)}$, M_α est un polynôme unitaire tel que $I(\alpha) = M_\alpha\mathbb{K}[X]$ car un polynôme quelconque est multiple de M si et seulement si ce polynôme est multiple de M_α.

Unicité de M_α**.** Si M_1 et M_2 sont deux polynômes non nuls et unitaires tels que $M_1\mathbb{K}[X] = M_2\mathbb{K}[X]$ alors M_1 divise M_2 et M_2 divise M_1. Par suite, il existe $k \in \mathbb{K}$ tel que $M_2 = kM_1$. Puisque d'autre part , M_1 et M_2 sont unitaires, $k = 1$ puis $M_1 = M_2$.

b) Si $P = M_\alpha$ alors $P(\alpha) = 0$. Vérifions de plus que M_α est irréductible sur $\mathbb{K}$. M_α n'est pas nul. Si il existe deux polynômes P_1 et P_2 tels que $M_\alpha = P_1P_2$ alors puisque $M_\alpha(\alpha) = 0$, on a $P_1(\alpha) = 0$ ou $P_2(\alpha) = 0$. On en déduit qu'un des deux polynômes P_1 ou P_2 est multiple de M_α et donc que l'autre est constant. On a montré que M_α est irréductible sur $\mathbb{K}$.
Réciproquement, si P est un polynôme unitaire et irréductible tel que $P(\alpha) = 0$ alors P est dans $I(\alpha)$ et donc multiple non nul de M_α. Par suite, il existe Q polynôme non nul tel que $P = M_\alpha Q$. Puisque P est irréductible sur $\mathbb{K}$ et que M_α n'est pas constant (une constante non nulle ne s'annulant pas en α, Q est constant. Enfin P et M_α étant unitaires, $Q = 1$ puis $P = M_\alpha$.

I-2) Le degré de α **sur** $\mathbb{K}$ **est égal à** 1
i/$\Rightarrow$ **ii**/ Si α est dans $\mathbb{K}$, $X - \alpha$ est dans $\mathbb{K}[X]$ et s'annule en α. M_α est un diviseur unitaire de ce polynôme et donc $M_\alpha = X - \alpha$. On en déduit que $d(\alpha, \mathbb{K}) = 1$.

ii/$\Rightarrow$ **i**/ Si $d(\alpha, \mathbb{K}) = 1$, M_α est unitaire de degré 1 et s'annule en α. Par suite, $M_\alpha = X - \alpha$ est dans $\mathbb{K}[X]$ ou encore α est dans $\mathbb{K}$.

i/$\Rightarrow$ **iii**/ Si α est dans $\mathbb{K}$, $\mathbb{K} \subset \mathbb{K}[\alpha] = \text{Vect}_{\mathbb{K}}\mathbb{K}(1, \alpha, \ldots) \subset \mathbb{K}$ et donc $\mathbb{K} = \mathbb{K}[\alpha]$.

iii/$\Rightarrow$**i**/ Si $\mathbb{K} = \mathbb{K}[\alpha]$, $\alpha = 0 \times 1 + 1 \times \alpha + 0 \times \alpha^2 + \ldots$ est dans $\mathbb{K}[\alpha] = \mathbb{K}$.

I-3) Le degré de α **sur** $\mathbb{K}$ **est égal à** 2
a) Soit α un nombre algébrique de degré 2 sur $\mathbb{K}$. D'après 2), α n'est pas dans $\mathbb{K}$ et donc la famille $(1, \alpha)$ est $\mathbb{K}$-libre.
Soit P un élément de $\mathbb{K}[X]$. La division euclidienne de P par M_α fournit des polynômes Q et R tels que $\deg(R) < \deg(M_\alpha) = 2$ et $P = QM_\alpha + R$. En prenant la valeur en α on obtient $P(\alpha) = R(\alpha)$.
Donc $\mathbb{K}[\alpha] = \{P(\alpha),\ P \in \mathbb{K}[X]\} = \{R(\alpha) / \ R \in \mathbb{K}_1[X]\} = \text{Vect}\mathbb{K}(1, \alpha)$. Donc $(1, \alpha)$ est une base de $\mathbb{K}[\alpha]$ et $\dim_{\mathbb{K}}\mathbb{K}[\alpha] = 2$.

Il est admis pour éviter une vérification ennuyeuse que $(\mathbb{K}[\alpha], +, \times)$ est un sous-anneau de $(\mathbb{R}[X], +, \times)$.
La seule chose à vérifier est alors : l'inverse dans $\mathbb{R}$ d'un élément non nul de $\mathbb{K}[\alpha]$ est dans $\mathbb{K}[\alpha]$.
Soit x un élément non nul de $\mathbb{K}[\alpha]$. Il existe un polynôme P tel que $x = P(\alpha)$ et $P \notin I(\alpha)$.
M_α étant irréductible sur $\mathbb{K}$, P et M_α sont premiers entre eux (dans le cas contraire, P serait multiple de M_α). Le théorème de Bézout fournit deux polynômes U et V tels que $UP + VM_\alpha = 1$. En prenant la valeur en α, on obtient $U(\alpha) \times x = 1$ et $\dfrac{1}{x} = U(\alpha)$ est bien dans $\mathbb{K}[\alpha]$.

$(\mathbb{K}[\alpha], +, \times)$ est donc un sous corps de $(\mathbb{R}[X], +, \times)$.

b) Posons $M_\alpha = X^2 + aX + b$ où a et b sont dans $\mathbb{K}$. M_α admet la racine réelle α et son discriminant est donc positif ou nul. Ce discriminant n'est pas nul car alors $\alpha = -\dfrac{a}{2}$ serait dans $\mathbb{K}$ ce qui n'est pas.

Le réel $\Delta = a^2 - 4b$ est donc un réel strictement positif de $\mathbb{K}$. De plus, $\alpha = -a \pm \sqrt{\Delta}$ est dans $\mathbb{K}[\sqrt{\Delta}]$ mais alors puisque $\mathbb{K}[\alpha]$ est une sous $\mathbb{K}$-algèbre de $(\mathbb{R}, +, \times)$ on a $\mathbb{K}[\alpha] \subset \mathbb{K}[\sqrt{\Delta}]$. De même $\sqrt{\Delta} = \pm(\alpha + a)$ est dans $\mathbb{K}[\alpha]$ et donc $\mathbb{K}[\sqrt{\Delta}] \subset \mathbb{K}[\alpha]$. Finalement, $\mathbb{K}[\alpha] = \mathbb{K}[\sqrt{k}]$ où k est un certain réel strictement positif de $\mathbb{K}$.

I-4) Le degré de α sur $\mathbb{K}$ est égal à un entier $n \geqslant 2$
a) On suppose que $d(\alpha, \mathbb{K}) = n \geqslant 2$.

Unicité. Si R_1 et R_2 sont deux polynômes de degrés au plus $n-1$ tels que $R_1(\alpha) = R_2(\alpha)$ alors le polynôme $R_1 - R_2$ est multiple de M_α de degré au plus $n-1$ et par définition de M_α et de n, $R_1 - R_2 = 0$.

Existence. Soit x dans $\mathbb{K}[\alpha]$. Il existe P dans $\mathbb{K}[X]$ tel que $x = P(\alpha)$. La division euclidienne de P par M_α fournit un polynôme Q et un polynôme R de degré inférieur ou égal à $n-1$ tel que $P = QM_\alpha + R$. En évaluant les deux membres de cette égalité en α, on obtient $x = R(\alpha)$ où cette fois-ci $\deg(R) < n$.

D'après ce qui précède, $\mathbb{K}[\alpha] = \mathrm{Vect}_{\mathbb{K}}(1, \alpha, ..., \alpha^{n-1})$. De plus $(1, \alpha, ..., \alpha_{n-1})$ est une famille $\mathbb{K}$-libre car s'il existe une combinaison linéaire nulle à coefficients dans $\mathbb{K}$ et non tous nuls de ces n réels, il existe alors un polynôme non nul de degré strictement plus petit que $n = \deg(M_\alpha)$ qui soit dans $I(\alpha)$ ce qui contredit la définition de M_α.

Finalement

$$\boxed{(1, \alpha, ..., \alpha^{n-1}) \text{ est une base du } \mathbb{K}\text{-espace vectoriel } \mathbb{K}[\alpha] \text{ et } \dim_{\mathbb{K}}(\mathbb{K}[\alpha]) = n = d(\alpha, \mathbb{K}).}$$

b) Soient x un élément non nul de $\mathbb{K}[\alpha]$ et R l'unique polynôme non nul de degré au plus $n-1$ tel que $x = R(\alpha)$.
Soit D un diviseur unitaire commun à R et M_α. D divise R et donc $\deg(D) < \deg(M_\alpha)$. Mais aussi D divise M_α et donc $D = 1$ car M_α est irréductible sur $\mathbb{K}$. R et M_α sont donc premiers entre eux.
Le théorème de Bézout fournit alors deux polynômes U et V tels que $UR + VM_\alpha = 1$ et en prenant la valeur en α, on obtient $U(\alpha)R(\alpha) = 1$.

c) D'après l'énoncé, il est admis que $(\mathbb{K}[\alpha], +, \times)$ est un sous anneau de $(\mathbb{R}, +, \times)$ et il reste à vérifier que l'inverse d'un élément x non nul de $\mathbb{K}[\alpha]$ est dans $\mathbb{K}[\alpha]$, mais ceci est démontré au c/.

$$\boxed{(\mathbb{K}[\alpha], +, \times) \text{ est un corps.}}$$

d) $(\mathbb{K}[\alpha], +, \times)$ est un sous-corps du corps $(\mathbb{R}, +, \times)$ contenant α et $\mathbb{K}$.
Soit L un sous-corps du corps $(\mathbb{R}, +, \times)$ contenant α et $\mathbb{K}$. L doit alors contenir 1, α, α^2,.. puis les produits de ces nombres par un élément de $\mathbb{K}$ puis les sommes de tels produits. En résumé, L contient $\mathbb{K}[\alpha]$.

$$\boxed{(\mathbb{K}[\alpha], +, \times) \text{ est le plus petit sous-corps du corps } (\mathbb{R}, +, \times) \text{ contenant } \alpha \text{ et } \mathbb{K}.}$$

I-5) Propriétés générales des polynômes P_n
a) Montrons par récurrence que pour tout entier naturel n, P_n est un polynôme de degré n et de coefficient dominant 2^n.
• $\deg(P_0) = 0$ et $\mathrm{dom}(P_0) = 1$ puis $\deg(P_1) = 1$ et $\mathrm{dom}(P_1) = 2$. L'affirmation est donc vraie quand $n = 0$ ou $n = 1$.
• Soit $n \geqslant 0$. Supposons que $\deg(P_n) = n$, $\mathrm{dom}(P_n) = 2^n$ puis $\deg(P_{n+1}) = n+1$, $\mathrm{dom}(P_{n+1}) = 2^{n+1}$.
Alors $\deg(P_{n+2}) = \deg(2XP_{n+1}) = n+2$ et $\mathrm{dom}(P_{n+2}) = \mathrm{dom}(2XP_{n+1}) = 2^{n+2}$.

On a montré par récurrence que

$$\boxed{\text{pour tout entier naturel } n, \ P_n \text{ est un polynôme de degré } n \text{ et de coefficient dominant } 2^n.}$$

• $P_2 = 2X(2X+1) - 1 = 4X^2 + 2X - 1$,
• $P_3 = 2X(4X^2 + 2X - 1) - (2X+1) = 8X^3 + 4X^2 - 4X - 1$,
• $P_4 = 2X(8X^3 + 4X^2 - 4X - 1) - (4X^2 + 2X - 1) = 16X^4 + 8X^3 - 12X^2 - 4X + 1$.

Ensuite, $Q_0 = 1$ et $Q_1 = X+1$ puis pour tout entier naturel n, $Q_{n+2} = (X+1)Q_{n+1} - Q_n$. Montrons alors par récurrence que pour tout entier naturel n, $Q_n \in \mathbb{Z}[X]$.
C'est vrai pour $n = 0$ et $n = 1$ et si pour $n \geqslant 0$, Q_n et Q_{n+1} sont dans $\mathbb{Z}[X]$, alors $Q_{n+2} = XQ_{n+1} - Q_n$ est dans $\mathbb{Z}[X]$. Le résultat est démontré par récurrence.

b) Q_n est à coefficients entiers, unitaire et par une récurrence immédiate a un coefficient constant a_0 égal à ± 1. Posons $Q_n = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ où $a_0 = \pm 1$.
Soit $x = \dfrac{p}{q}$ une racine rationnelle de Q_n où $q \in \mathbb{N}^*$ et $p \in \mathbb{Z}^*$ (car $a_0 \neq 0$) et $p \wedge q = 1$. L'égalité $Q_n\left(\dfrac{p}{q}\right) = 0$ fournit après réduction au même dénominateur $p^n + a_{n-1}p^{n-1}q + ... + a_1pq^{n-1} + a_0q^n$ et donc les deux égalités :

$$(1)\ p^n = q(-a_{n-1}p^{n-1} - a_{n-2}p^{n-2}q ... - a_0q^{n-1}) \text{ et } (2)\ a_0q^n = p(-a_1q^{n-1} ... - a_{n-1}qp^{n-2} - p^{n-1}).$$

D'après (1), q divise p^n et puisque p^n et q sont premiers entre eux, le théorème de Gauss montre que q divise 1 puis que $q = 1$.
D'après (2), p divise $a_0 q^n$ et puisque p et q^n sont premiers entre eux le théorème de GAUSS montre que p divise $a_0 = \pm 1$ puis que $p = \pm 1$.
Finalement, si x est une racine rationnelle de Q_n, alors $x = 1$ ou $x = -1$.

Soit $n \in \mathbb{N}$. $Q_{n+3} + XQ_n = XQ_{n+2} - Q_{n+1} + XQ_n = X(Q_{n+2} + Q_n) - Q_{n+1} = (X^2 - 1)Q_{n+1}$.
Si x est une racine rationnelle de l'un des polynômes Q on sait que $x \in \{-1, 1\}$ et donc $x^2 - 1 = 0$. On en déduit que pour tout entier naturel n, $Q_{n+3}(x) + xQ_n(x) = (x^2 - 1)Q_{n+1}(x)$.
Donc x est une racine rationnelle de Q_{n+3} si et seulement si x est une racine rationnelle de $-XQ_n$ ce qui équivaut à x est une racine rationnelle de Q_n car $x \neq 0$.

Q_n et Q_{n+3} ont même ensemble de racines rationnelles.

• Q_0 n'a pas de racine rationnelle donc pour $n \in \mathbb{N}$, Q_{3n} n'a pas de racine rationnelle. Il en est de même pour P_{3n} (puisque les racines de Q_{3n} sont les doubles des racines de P_{3n}).
• Q_1 admet -1 pour unique racine rationnelle et donc, pour tout entier naturel n, P_{3n+1} admet $-\dfrac{1}{2}$ pour unique racine rationnelle.
• Q_2 n'admet pas de racine rationnelle et donc, pour tout entier naturel n, P_{3n+2} n'admet pas de racine rationnelle.

$\forall n \in \mathbb{N}$, P_{3n} et P_{3n+2} n'ont pas de racine rationnelle et P_{3n+1} admet $-\dfrac{1}{2}$ pour unique racine rationnelle.

I-6) Racines des polynômes P_n
a) L'équation caractéristique de la récurrence proposée est $z^2 - 2z\cos(\theta) + 1 = 0$ qui s'écrit encore $(z - e^{i\theta})(z - e^{-i\theta}) = 0$.
Puisque θ est dans $]0, \pi[$, cette équation est à racines simples et une base de l'espace des solutions est $\left(\left(e^{in\theta}\right)_{n\in\mathbb{N}}, \left(e^{-in\theta}\right)_{n\in\mathbb{N}}\right)$.
Une autre base est $\left((\cos(n\theta))_{n\in\mathbb{N}}, (\sin(n\theta)_{n\in\mathbb{N}}\right)$ ou encore, il existe deux réels λ et μ tels que pour tout entier naturel n, on ait :

$$u_n = \lambda\cos(n\theta) + \mu\sin(n\theta).$$

$n = 0$ fournit $\lambda = u_0$ et $n = 1$ fournit $u_1 = \lambda\cos(\theta) + \mu\sin(\theta)$ et donc $\mu = \dfrac{u_1 - u_0\cos(\theta)}{\sin(\theta)}$.

$$\forall n \in \mathbb{N},\ u_n = u_0\cos(n\theta) + \frac{u_1 - u_0\cos(\theta)}{\sin(\theta)}\sin(n\theta).$$

b) $v_0 = P_0(\cos(\theta)) = 1$ et $v_1 = 2\cos(\theta) + 1$ puis pour $n \in \mathbb{N}$

$$v_{n+2} = P_{n+2}(\cos(\theta)) = 2P_{n+1}(\cos(\theta))\cos(\theta) - P_n(\cos(\theta)) = 2v_{n+1}\cos(\theta) - v_n.$$

Si θ est dans $]0, \pi[$, d'après ce qui précède, pour tout entier naturel n

$$v_n = \cos(n\theta) + \frac{2\cos(\theta) + 1 - \cos(\theta)}{\sin(\theta)}\sin(n\theta) = \frac{\sin((n+1)\theta) + \sin(n\theta)}{\sin(\theta)}.$$

$$\forall n \in \mathbb{N},\ P_n(\cos(\theta)) = \frac{\sin((n+1)\theta) + \sin(n\theta)}{\sin(\theta)}.$$

Soit $n \in \mathbb{N}^*$. Pour θ dans $]0, \pi[$,

$$P_n(\cos(\theta)) = 0 \Leftrightarrow \sin((n+1)\theta) + \sin(n\theta) = 0 \Leftarrow \exists k \in \mathbb{Z}/\ (n+1)\theta = -n\theta + 2k\pi \Leftarrow \exists k \in [\![1, n]\!]/\ \theta = \frac{2k\pi}{2n+1}.$$

Pour $k \in [\![1, n]\!]$, posons $\theta_{k,n} = \dfrac{2k\pi}{2n+1}$. Pour $k \in [\![1, n]\!]$, $\theta_{k,n}$ est dans $]0, \pi[$ et donc les n nombres $x_{k,n} = \cos\left(\dfrac{2k\pi}{2n+1}\right)$ sont deux à deux distincts et racines de P_n qui est de degré n.
On a donc trouvé toutes les racines de P_n à savoir les $x_{k,n} = \cos\left(\dfrac{2k\pi}{2n+1}\right)$, $1 \leqslant k \leqslant n$. Ces racines sont réelles simples et dans $]-1, 1[$.

$$\forall n \in \mathbb{N}^*, \text{ les racines de } P_n \text{ sont les } x_{k,n} = \cos\left(\frac{2k\pi}{2n+1}\right),\ 1 \leqslant k \leqslant n.$$

c) $\cos\left(\frac{2\pi}{5}\right) = x_{1,2}$, $\cos\left(\frac{2\pi}{7}\right) = x_{1,3}$, et $\cos\left(\frac{2\pi}{9}\right) = x_{1,4}$ sont respectivement racines de P_2, P_3 et P_4 qui sont à coefficients rationnels et ces trois nombres sont algébriques.

$\cos\left(\frac{2\pi}{5}\right)$ est racine du polynôme $P_2 = 4X^2 + 2X - 1$ et donc est de degré inférieur ou égal à 2. Mais $4X^2 + 2X - 1$ n'a pas de racines rationnelles donc

$$\boxed{d\left(\cos\left(\frac{2\pi}{5}\right), \mathbb{Q}\right) = 2 \text{ et } M_{\cos(2\pi/5)} = X^2 + \frac{1}{2}X - \frac{1}{4}.}$$

$\cos\left(\frac{2\pi}{7}\right)$ est racine du polynôme $P_3 = 8X^3 + 4X^2 - 4X - 1$ et donc est de degré inférieur ou égal à 3. Si le polynôme $8X^3 + 4X^2 - 4X - 1$ n'est pas irréductible sur $\mathbb{Q}$, il est divisible par un polynôme de degré 1 à coefficients dans $\mathbb{Q}$ et a donc une racine rationnelle ce qui n'est pas d'après la question 5)b). Donc ce polynôme est irréductible sur $\mathbb{Q}$.

$$\boxed{d\left(\cos\left(\frac{2\pi}{7}\right), \mathbb{Q}\right) = 3 \text{ et } M_{\cos(2\pi/7)} = X^3 + \frac{1}{2}X^2 - \frac{1}{2}X - \frac{1}{8}.}$$

$\cos\left(\frac{2\pi}{9}\right)$ est racine du polynôme $P_4 = 16X^4 + 8X^3 - 12X^2 - 4X + 1$. Ce polynôme admet $-\frac{1}{2}$ pour racine d'après 5)b) et n'est pas irréductible sur $\mathbb{Q}$. Comme $16X^4 + 8X^3 - 12X^2 - 4X + 1 = (2X+1)(8X^3 - 6X + 1)$ et que $\cos\left(\frac{2\pi}{9}\right)$ n'est pas $-\frac{1}{2}$, le polynôme minimal de $\cos\left(\frac{2\pi}{9}\right)$ est un diviseur irréductible de $8X^3 - 6X + 1$. Mais ce dernier polynôme est irréductible sur $\mathbb{Q}$ car sinon ce polynôme admettrait une racine rationnelle, nécessairement égale à $-\frac{1}{2}$ ce qui n'est pas.

$$\boxed{d\left(\cos\left(\frac{2\pi}{9}\right), \mathbb{Q}\right) = 3 \text{ et } M_{\cos(2\pi/9)} = X^3 + \frac{3}{4}X + \frac{1}{8}.}$$

I-7) a) Soit $\alpha = \cos\left(\frac{2\pi}{9}\right)$. D'après les questions 6)c) et 4)a), $\mathbb{Q}[\alpha]$ est de dimension 3 sur $\mathbb{Q}$ et une base de $\mathbb{Q}[\alpha]$ est $(1, \alpha, \alpha^2)$.

$\cos\left(\frac{4\pi}{9}\right) = 2\cos^2\left(\frac{2\pi}{9}\right) - 1$ et donc $\cos\left(\frac{4\pi}{9}\right) = -1 + 2\alpha^2$.

$\cos\left(\frac{8\pi}{9}\right) = 2(2\alpha^2 - 1)^2 - 1 = 8\alpha^4 - 8\alpha^2 + 1$.

La division euclidienne de $8X^4 - 8X^2 + 1$ par $8X^3 - 6X + 1$ s'écrit

$$8X^4 - 8X^2 + 1 = X(8X^3 - 6X + 1) - 2X^2 - X + 1,$$

et en évaluant en α, on obtient $\cos\left(\frac{8\pi}{9}\right) = 1 - \alpha - 2\alpha^2$.

$$\boxed{\cos\left(\frac{4\pi}{9}\right) = -1 + 2\alpha^2 \text{ et } \cos\left(\frac{8\pi}{9}\right) = 1 - \alpha - 2\alpha^2.}$$

b) L'égalité $f(1)^2 = f(1)$ montre que $f(1) = 0$ ou $f(1) = 1$. $f(1) = 0$ fournit pour tout x de $\mathbb{Q}[\alpha]$, $f(x) = f(x) \times f(1) = 0$ et donc $f = 0$ ce qui n'est pas. Donc, $f(1) = 1$, puis si $x \in \mathbb{Q}$, $f(x) = xf(1) = x$ (car f est $\mathbb{Q}$-linéaire).

Ensuite, $0 = f(0) = f(8\alpha^3 - 6\alpha + 1) = 8f(\alpha)^3 - 6f(\alpha) + 1$. Donc $f(\alpha)$ est l'une des trois racines du polynôme $8X^3 - 6X + 1$ à savoir, d'après la question 6)b), $f(\alpha) = \alpha = \cos\left(\frac{2\pi}{9}\right)$ ou $f(\alpha) = \cos\left(\frac{4\pi}{9}\right) = -1 + 2\alpha^2$ ou $f(\alpha) = \cos\left(\frac{8\pi}{9}\right) = 1 - \alpha - 2\alpha^2$.

Par suite, puisque l'endomorphisme f est entièrement par l'image $(f(1), f(\alpha), f(\alpha)^2)$ de la base $(1, \alpha, \alpha^2)$, il existe au plus trois endomorphismes d'algèbre solutions.

Réciproquement,

1er cas. Si $f(\alpha) = \alpha$ et donc $f(\alpha^2) = f(\alpha)^2 = \alpha^2$, f coïncide avec Id sur une base de $\mathbb{Q}[\alpha]$. Donc $f = Id$ qui est bien solution.

2ème cas. Soit β une racine du polynôme $8X^3 - 6X + 1$ distincte de α (c'est-à-dire $\beta = \cos\left(\frac{4\pi}{9}\right)$ ou $\beta = \cos\left(\frac{8\pi}{9}\right)$).

On définit un unique endomorphisme f du $\mathbb{Q}$-espace $\mathbb{Q}[\alpha]$ en posant $f(1)=1$, $f(\alpha)=\beta$ et $f(\alpha^2)=\beta^2$ (pour a, b et c rationnels, $f(a+b\alpha+c\alpha^2)=a+b\beta+c\beta^2$). Il reste encore vérifier que pour tout (x,y) de $\mathbb{Q}[\alpha]$, on a $f(xy)=f(x)f(y)$. Par $\mathbb{Q}$-linéarité de f, il suffit de vérifier ces égalités sur une base de $\mathbb{Q}[\alpha]$ ou encore de vérifier que $f(\alpha^k\alpha^l)=f(\alpha^k)f(\alpha^l)$ pour k et l éléments de $\{0,1,2\}$. Parmi ces neuf égalités, il en reste trois à vérifier à savoir $f(\alpha^3)=f(\alpha)f(\alpha^2)$ et $f(\alpha^4)=f(\alpha)f(\alpha^3)=f(\alpha^2)^2$ ce qui se résume encore aux deux vérifications $f(\alpha^3)=\beta^3$ et $f(\alpha^4)=\beta^4$. Mais $f(\alpha^3)=f\left(\dfrac{6\alpha-1}{8}\right)=\dfrac{6\beta-1}{8}=\beta^3$ et $f(\alpha^4)=f\left(\dfrac{6\alpha^2-\alpha}{8}\right)=\dfrac{6\beta^2-\beta}{8}=\beta^4$. Donc on obtient bien deux autres endomorphismes solutions.
On a trouvé trois endomorphismes non nuls solutions $f_1=Id$ et f_2 et f_3 entièrement déterminés par les égalités $f_2\left(\cos\left(\dfrac{2\pi}{9}\right)\right)=\cos\left(\dfrac{4\pi}{9}\right)$ et $f_3\left(\cos\left(\dfrac{2\pi}{9}\right)\right)=\cos\left(\dfrac{8\pi}{9}\right)$.

Matrices M_1, M_2 et M_3 de ces endomorphismes dans la base B. $f_1=Id$ et donc $M_1=I_3$.
$f_2(1)=1$, $f_2(\alpha)=-1+2\alpha^2$ et $f_2(\alpha^2)=4\alpha^4-4\alpha^2+1=\dfrac{\alpha}{2}(8\alpha^3-6\alpha+1)-\alpha^2-\dfrac{\alpha}{2}+1=-\alpha^2-\dfrac{\alpha}{2}+1$ et donc $M_2=\begin{pmatrix}1&-1&1\\0&0&-1/2\\0&2&-1\end{pmatrix}$
$f_3(1)=1$, $f_3(\alpha)=1-\alpha-2\alpha^2$ et

$$f_3(\alpha^2)=(1-\alpha-2\alpha^2)^2=4\alpha^4+4\alpha^3-3\alpha^2-2\alpha+1=\left(\frac{\alpha}{2}+\frac{1}{2}\right)(8\alpha^3-6\alpha+1)+\frac{1}{2}\alpha+\frac{1}{2}=\frac{1}{2}+\frac{1}{2}\alpha,$$

et donc $M_3=\begin{pmatrix}1&1&1/2\\0&-1&1/2\\0&-2&0\end{pmatrix}$. Les trois matrices cherchées sont

$$\boxed{M_1=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix},\ M_2=\begin{pmatrix}1&-1&1\\0&0&-1/2\\0&2&-1\end{pmatrix}\text{ et }M_3=\begin{pmatrix}1&1&1/2\\0&-1&1/2\\0&-2&0\end{pmatrix}.}$$

f_1, f_2 et f_3 ont tous les trois un déterminant égal à 1 et sont donc des automorphismes de l'espace vectoriel $\mathbb{Q}[\alpha]$. Donc $\{f_1,f_2,f_3\}$ une partie non vide de $GL(\mathbb{Q}[\alpha])$, évidemment stable pout la loi $\circ$ et le passage à l'inverse (en revenant à la définition de f_1, f_2 et f_3) et donc un sous groupe de $(GL(\mathbb{Q}[\alpha]),\circ)$.

I-8) Exemple de nombres transcendants sur $\mathbb{Q}$
a) S est de degré supérieur ou égal à 2 irréductible sur $\mathbb{Q}$ et n'admet donc pas de racines rationnelles.
Posons $S=a_nX^n+...+a_0$. Soit C_S le PGCD des dénominateurs des rationnels a_0,..., a_n. $C_S\left|q_nS\left(\dfrac{p}{q}\right)\right|$ est un entier naturel qui ne peut être nul car S n'a pas de racine rationnelle. Donc $C_S\left|q_nS\left(\dfrac{p}{q}\right)\right|\geqslant 1$ pour tout entier relatif p et tout entier naturel non nul q.

b) Soit α une racine de S. Donc $S(\alpha)=0$ et si $r=\dfrac{p}{q}$ est élément de $[\alpha-1,\alpha+1]$, on a d'après l'inégalité des accroissements finis

$$\frac{1}{C_Sq^n}\leqslant|S(r)|=|S(r)-S(\alpha)|\leqslant\left(\sup_{t\in[\alpha-1,\alpha+1]}|S'(t)|\right)|r-\alpha|.$$

On ne peut avoir $\sup\limits_{t\in[\alpha-1,\alpha+1]}|S'(t)|=\max\limits_{t\in[\alpha-1,\alpha+1]}|S'(t)|=0$ car S' a un nombre fini de racines et donc $K=\dfrac{1}{C_S\max\limits_{t\in[\alpha-1,\alpha+1]}|S'(t)|}$ convient (un nombre algébrique ne peut en un certain sens pas être approché de trop près par un rationnel).

c) Pour $k\in\mathbb{N}$, soit $u_k=\dfrac{1}{10^{k!}}$. Alors pour $k\geqslant 0$, $0\leqslant u_k\leqslant\dfrac{1}{10^k}$ terme général d'une série géométrique convergente et donc la suite (t_n) converge (vers le réel $t=0,21000100....$)

Pour n entier naturel donné, $|t-t_n|=\sum\limits_{k=n+1}^{+\infty}\dfrac{1}{10^{k!}}=10^{-(n+1)!}\sum\limits_{k=n+1}^{+\infty}\dfrac{1}{10^{k!-(n+1)!}}$.
Mais pour $k\geqslant n+1$, $10^{-k!+(n+1)!}\leqslant 2^{-k!+(n+1)!}\leqslant 2^{-k+n+1}$ car pour $k\geqslant n+2$, $k!-(n+1)!=(n+1)!((n+2)...k-1)\geqslant k-1\geqslant k-n-1$ et donc $\sum\limits_{k=n+1}^{+\infty}\dfrac{1}{10^{k!-(n+1)!}}\leqslant\sum\limits_{k=n+1}^{+\infty}\dfrac{1}{2^{k-n-1}}=2$. En résumé

$$\forall n\in\mathbb{N},\ |t-t_n|\leqslant\frac{2}{10^{(n+1)!}}.$$

Si t était algébrique de degré $m > 1$, on aurait pour tout rationnel $r = \frac{p}{q}$ de $[t-1, t+1]$, $|t-r| \geqslant \frac{K}{q^m}$ (en appliquant b/ au polynôme minimal de t).

Mais pour tout entier n, on a $|t - t_n| \leqslant \frac{2}{10^{(n+1)!}} \leqslant 1$ et puisque t_n est un rationnel de dénominateur $10^{n!}$, on aurait pour tout entier naturel n, $\frac{K}{10^{m \times n!}} \leqslant |t - t_n| \leqslant 2 \times 10^{-(n+1)!}$ ou encore $2 \times 10^{-((n+1)-m)n!} \geqslant K > 0$. Ceci est absurde car à m fixé, $2 \times 10^{-((n+1)-m)n!}$ tend vers 0 quand n tend vers l'infini. Donc

t est transcendant sur $\mathbb{Q}$.

Remarque historique. Le b) est le théorème de Liouville (1809-1882) et permet de démontrer que les nombres de Liouville (c'est-à-dire les nombres de la forme $\sum_{n=0}^{+\infty} \frac{c_n}{10^{n!}}$ où les c_n sont des chiffres et la suite $(c_n)_{n\in\mathbb{N}}$ n'est pas nulle à partir d'un certain rang) sont transcendants. Ce sont les premiers nombres transcendants historiquement connus (l'existence de nombres transcendants est assurée par le fait que l'ensemble des nombres algébriques est dénombrable et que $\mathbb{R}$ ne l'est pas) mais ils sont construits artificiellement dans ce but. e ou π ne sont pas des nombres de Liouville. Hermite a démontré en 1873 que e est transcendant et Lindemann a démontré en 1882 que π est transcendant.)

Deuxième partie

II-1) Intersection de droites et de cercles appartenant à D ou à C

a) Soient (x_1, y_1) et (x_2, y_2) deux points distints à coordonnées dans $\mathbb{K}$ et $\mathscr{D}$ la droite passant par ces deux points. Une équation de $\mathscr{D}$ est

$$(y_2 - y_1)(x - x_1) - (x_2 - x_1)(y - x_1) = 0.$$

On vient de fournir une équation de $\mathscr{D}$ à coefficients dans $\mathbb{K}$.

b) Soient Ω un point à coordonnées dans $\mathbb{K}$ et R la distance entre deux points dont les coordonnées sont dans $\mathbb{K}$. Soient enfin $\mathscr{C}$ le cercle ce centre Ω et de rayon R. Alors R^2 est dans $\mathbb{K}$ et $(x - x_\Omega)^2 + (y - y_\Omega)^2 = R^2$ est une équation de $\mathscr{C}$ à coefficients dans $\mathbb{K}$.

c) Soient $\mathscr{D}_1$ et $\mathscr{D}_2$ deux droites sécantes de D. Elles admettent toutes deux une équation dont les coefficients sont dans $\mathbb{K}$. Les coordonnées du point d'intersection de ces deux droites sont d'après les formules de Cramer des rapports d'éléments de $\mathbb{K}$ et donc sont dans $\mathbb{K}$.

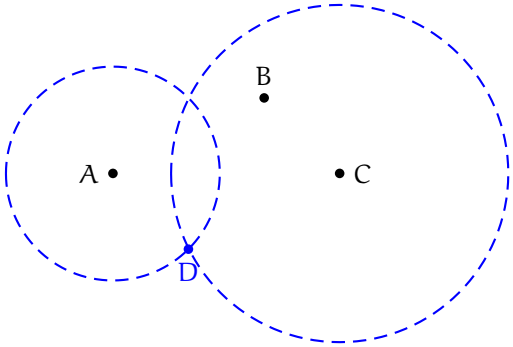
d) Soient $\mathscr{D} : ax + by + c = 0$ une droite de D et $\mathscr{C} : x^2 + y^2 + ux + vy + w = 0$ un cercle de C (a, b, u, v, w étant dans $\mathbb{K}$). En supposant par exemple $b \neq 0$ (on a $a \neq 0$ ou $b \neq 0$), si (x, y) est commun à C et D alors $y = -\frac{a}{b}x - \frac{c}{b}$ puis :

$$x^2 + \left(-\frac{a}{b}x - \frac{c}{b}\right)^2 + ux + v\left(-\frac{a}{b}x - \frac{c}{b}\right) + w = 0,$$

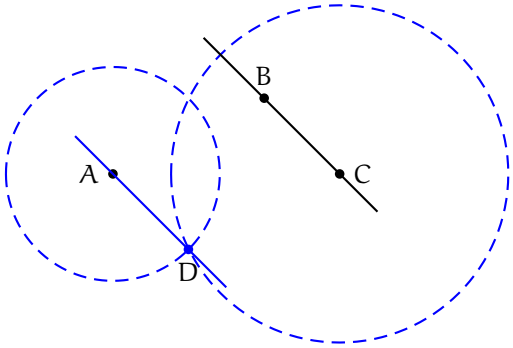
qui est une équation du second degré à coefficients dans $\mathbb{K}$ qui admet par définition des solutions réelles. x (puis y) est alors dans $\mathbb{K}[\sqrt{\Delta}]$ (où Δ est le discriminant de l'équation précédente) qui est soit $\mathbb{K}$, soit une extension quadratique de $\mathbb{K}$.

e) Les coordonnées d'un point commun à deux cercles de C sont soit dans $\mathbb{K}$, soit dans une même extension quadratique de $\mathbb{K}$ car déterminer l'intersection de deux cercles équivaut en retranchant une des deux équations à l'autre à déterminer l'intersection d'un cercle et d'une droite dont les coefficients des équations restent dans le même corps.

II-2) a) Le point D tel que ABCD est un parallèlogramme est à la fois sur le cercle de centre A et de rayon BC et sur le cercle de centre C et de rayon AB. Donc D est constructible à partir de A, B et C.



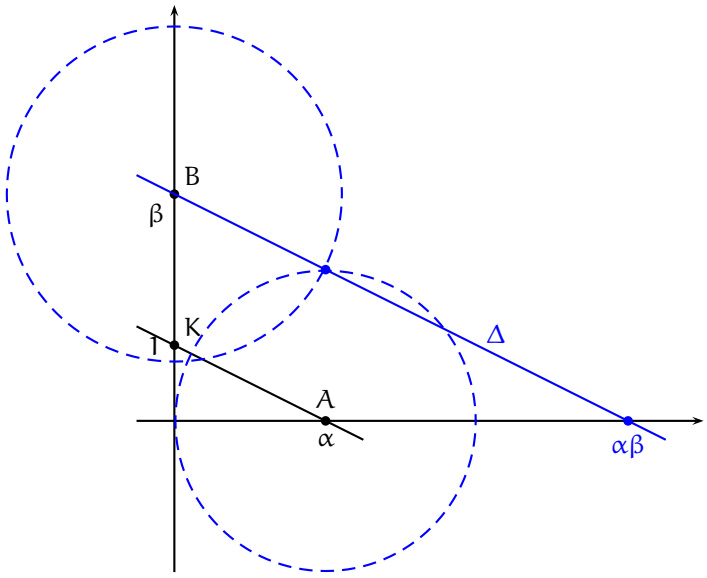
Soient A, B et C trois points distincts et non alignés et Δ la droite passant par B et C. La parallèle à Δ passant par A est la droite passant par A et le point D tel que ABCD soit un parallélogramme. Elle est constructible à partir de A, B et C.



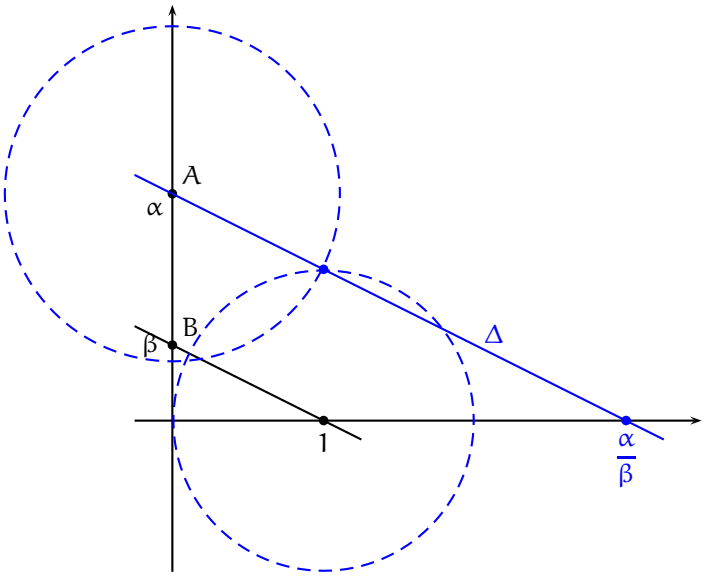
b) J est l'intersection de la droite (OI) et du cercle de centre O et de rayon $1 = OI$. Le point J est donc constructible puis en réitérant, on obtient tous les points de(Ox) dont l'abscisse est un entier relatif.
On construit ensuite K' intersection du cercle de centre I et de rayon IJ et du cercle de centre J et de rayon IJ. K' est constructible à partir de O et I, est sur (Oy) et distinct de O. K est alors l'intersection de la droite (OK') et du cercle de centre I et de rayon OI. Mais alors sont également constructibles à partir de O et I, tous les points de (Oy) dont l'ordonnée est un entier relatif.
On obtient plus généralement le point de coordonnées (m, n) où m et n sont des entiers relatifs comme intersection du cercle de centre $M(m, 0)$ et de rayon $ON = |n|$ où $N(0, n)$ et du cercle de centre $N(0, n)$ et de rayon $OM = |m|$.
Sont maintenant constructibles à la règle et au compas tous les points à coordonnées entières et on redémarre avec ce stock de points.

Somme de deux nombres constructibles. Soient α et β des réels strictement positifs constructibles. Les points $A(\alpha, 0)$ et $B(-\beta, 0)$ sont constructibles. Le point $C(\alpha + \beta, 0)$ est le point d'intersection de la droite (Ox) et du cercle de centre O et de rayon AB. Le point C est donc constructible ou ce qui revient au même le réel $\alpha + \beta$ est constructible.

Produit de deux nombres constructibles. Soient α et β deux réels strictement positifs et constructibles. Alors les points $A(\alpha, 0)$ et $B(0, \beta)$ sont des points constructibles.
D'après le théorème de Thales, si $K(0, 1)$, la parallèle Δ à la droite (AK) passant par B coupe la droite (OI) en le point de coordonnées $(\alpha\beta, 0)$. Le réel $\alpha\beta$ est donc constructible.

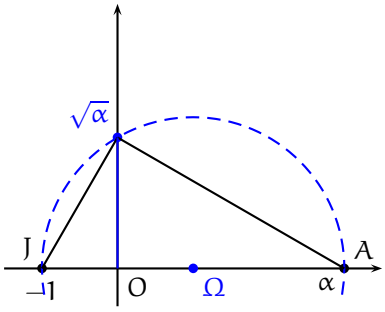


Quotient de deux nombres constructibles (et inverse d'un nombre constructible). On adapte la construction précédente en échangeant les rôles de α, β et 1. La construction de $\frac{\alpha}{\beta}$ fournit en particulier une construction de l'inverse d'un nombre strictement positif constructible.



Le travail précédent montre qu'en partant de O et I, on arrive à construire tous les points dont les coordonnées sont des nombres rationnels.

Racine carrée d'un nombre constructible). Soit α un réel strictement positif constructible.
On sait que dans un triangle MNP rectangle en M, si H est le pied de la hauteur issue de M alors $MH^2 = HN \times HP$.
On prend $J(-1,0)$, $O(0,0)$ et $A(\alpha,0)$ puis on construit le milieu Ω du segment [AJ] (le réel $\frac{\alpha-1}{2}$ est constructible).
Le point d'intersection du cercle de centre Ω passant par A et de la droite (Oy) est un point R tel que AJR est rectangle en R et puisque $OR^2 = OJ \times OA$, le point R est le point $(0,\sqrt{\alpha})$. Le réel $\sqrt{\alpha}$ est constructible si α l'est.



II-3) Une condition nécessaire et suffisante de constructibilité

a) Soit M un point constructible. Soient M_1,..., M_p tels que
- M_1 est construit à partir de O et I (donc M_1 est soit O, soit I, soit J)
- $\forall i \in [\![2,p]\!]$, M_i est construit à partir de $\{O, I, M_1, ..., M_{i-1}\}$
- $M_p = M$.

Les cordonnées de M_1 sont soit dans un corps $\mathbb{K}'_1$ qui est d'après la question II-1) soit $\mathbb{Q}$, soit une extension quadratique de $\mathbb{Q}$.
De même les cordonnées de M_2 sont dans un corps $\mathbb{K}'_2$ qui est soit $\mathbb{K}'_1$, soit une extension quadratique de $\mathbb{K}'_1$ ...
On construit ainsi une suite finie de corps $\mathbb{K}'_0 = \mathbb{Q} \subset \mathbb{K}'_1 \subset ... \subset \mathbb{K}'_p$ tels que $\mathbb{K}'_i$ est soit $\mathbb{K}'_{i-1}$, soit une extension quadratique de $\mathbb{K}'_{i-1}$ et les cordonnées de M sont dans $\mathbb{K}'_p$.
En éliminant les étapes où on n'agrandit pas le corps, on a construit une suite de corps $\mathbb{K}_0 \subset \mathbb{K}_1 ... \subset \mathbb{K}_n$ tels que $\mathbb{K}_0 = \mathbb{Q}$, chaque $\mathbb{K}_i$ est une extension quadratique de $\mathbb{K}_{i-1}$ et les cordonnées de M sont dans $\mathbb{K}_n$.

b) Si M a ses coordonnées dans $\mathbb{Q} = \mathbb{K}_0$, M est constructible d'après la question 2).
Soit $n \in \mathbb{N}$. Supposons que si un point a ses cordonnées dans $\mathbb{K}_n$ alors ce point est constructible.
Soit M un point dont les coordonnées sont dans $\mathbb{K}_{n+1}$. On sait que d'après I-3) que les coordonées de M sont de la forme $a + b\sqrt{alpha}$ où a, b et α sont dans $\mathbb{K}_n$. Mais alors la question II-2)b) montre que M est constructible.
Le résultat est démontré par récurrence.

En résumé, un point M est constructible si et seulement si il existe une suite finie de corps $\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 ... \subset \mathbb{K}_n$ où chaque corps est entension quadratique du précédent et où M a ses coordonnées dans $\mathbb{K}_n$.

En particulier, un nombre transcendant n'est pas constructible à la règle et au compas. C'est le cas de π qui n'est pas constructible à la règle et au compas et rend vaine la recherche d'une solution au problème de la quadrature du cercle.

II-4) Une condition nécessaire de constructibilité

a) Soient $(e_i)_{1 \leqslant i \leqslant q}$ une base du F-espace vectoriel G et $(f_j)_{1 \leqslant j \leqslant r}$ une base du G-espace vectoriel H. Alors
$H = \text{Vect}_F(e_i f_j)_{1 \leqslant i \leqslant q,\ 1 \leqslant j \leqslant r}$ et H est un F-espace vectoriel de dimension finie inférieure ou égale à qr.

De plus si $(\lambda_{i,j})_{1\leqslant i\leqslant q,\ 1\leqslant j\leqslant r}$ est une famille de qr éléments de F,

$$\sum_{1\leqslant i\leqslant q,\ 1\leqslant j\leqslant r}\lambda_{i,j}e_if_j=0\Rightarrow\sum_{j=1}^{r}\left(\sum_{i=1}^{q}\lambda_{i,j}e_i\right)f_j=0$$

$$\Rightarrow\forall j\in[\![1,r]\!],\ \sum_{i=1}^{q}\lambda_{i,j}e_i=0 \text{ (car la famille } (f_j)_{1\leqslant j\leqslant r} \text{ est } G\text{-libre)}$$

$$\Rightarrow\forall(i,j)\in[\![1,q]\!]\times[\![1,r]\!],\ \lambda_{i,j}=0 \text{ (car la famille } (e_i)_{1\leqslant j\leqslant q} \text{ est } F\text{-libre).}$$

Finalement, la famille $(e_if_j)_{1\leqslant i\leqslant q,\ 1\leqslant j\leqslant r}$ est une base du F- espace vectoriel H et

$$\boxed{\dim_F H=(\dim_G H)\times(\dim_F G).}$$

b) Mais alors immédiatement $\dim_{\mathbb{Q}}\mathbb{K}_n=2^n$.

c) Soit α un réel constructible. Cela signifie que $\mathbb{Q}[\alpha]$ est contenu dans un certain $\mathbb{K}_n$ de dimension 2^n sur $\mathbb{Q}$. D'après la question précédente, la dimension de $\mathbb{Q}[\alpha]$ sur $\mathbb{Q}$ est un diviseur de 2^n et donc une puissance de 2. On a montré que

$$\boxed{\text{Si } \alpha \text{ est constructible, son degré sur } \mathbb{Q} \text{ est nécessairement une puissance de 2.}}$$

II-5) Polygones réguliers constructibles

Le triangle équilatéral et le carré sont constructibles puis en bissectant, l'hexagone et l'octogone sont constructibles . Comme $\cos\left(\frac{2\pi}{5}\right)=\frac{-1+\sqrt{5}}{4}$ est constructible (étant dans une extension quadratique de $\mathbb{Q}$) , le pentagone régulier est constructible de même que le décagone.

$\cos\left(\frac{2\pi}{7}\right)$ et $\cos\left(\frac{2\pi}{9}\right)$ sont de degré 3 sur $\mathbb{Q}$ et donc non constructibles et l'heptagone et le nonagone ne sont pas constructibles à la règle et au compas.

Remarque. Gauss a démontré que le polygone régulier à n cotés est constructible à la règle et au compas si et seulement si la décomposition de n en facteurs premiers est de la forme $2^\alpha p_1...p_s$ où les p_k sont des nombres premiers de Fermat (c'est-à-dire de la forme $2^{2^k}+1$).

Sont ainsi constructibles les polygones à 3, 4, 5, 6, 8, 10, 12, 15, 16, 17 et 20 (icosagone) côtés.

