Deuxième épreuve : option M.

CORRIGE

I.1°. a. Le produit d'un polynôme P appartenant au sous-espace vectoriel $\mathfrak{J}(\alpha)$ de $\mathbb{K}[X]$ appartient à $\mathfrak{J}(\alpha)$. C'est donc un idéal de $\mathbb{K}[X]$. Or tout idéal de $\mathbb{K}[X]$ autre que $\mathbb{K}[X]$ est principal. Par suite les éléments de $\mathfrak{J}(\alpha)$ sont proportionnels à un même polynôme M_α qui, s'il est supposé unitaire, est unique.

b . *La condition est nécessaire* :

Puisque le polynôme M_α appartient à $\mathfrak{J}(\alpha)$, $M_\alpha(\alpha) = 0$. Si M_α n'était pas irréductible dans $\mathbb{K}[X]$, il existerait deux polynômes P et Q dans $\mathbb{K}[X]$ tels que :

$$M_\alpha = Q.P ,$$

avec $d°Q \geq 1$; $d°P \geq 1$; donc $Q(\alpha) = 0$ ou $P(\alpha) = 0$. Par suite M_α ne serait pas le polynôme unitaire de $\mathfrak{J}(\alpha)$ de plus bas degré.

La condition est suffisante :

Soit P un polynôme unitaire de $\mathbb{K}[X]$ admettant α comme racine et irréductible dans $\mathbb{K}[X]$. Il appartient sûrement à $\mathfrak{J}(\alpha)$; il est donc divisible par M_α. Or P est supposé irréductible ; donc : $P = M_\alpha$.

I.2°. Démontrons les implications suivantes :

• i/ $\Rightarrow$ ii/

Si $\alpha \in \mathbb{K}$; le polynôme minimal est $X - \alpha$; le degré de α est donc égal à 1.

• ii/ $\Rightarrow$ i/

Si $d(\alpha, \mathbb{K}) = 1$, le polynôme minimal unitaire est de degré égal à 1 et admet α comme racine ; par suite : $M_\alpha = X - \alpha$. Puisque $M_\alpha \in \mathbb{K}[X]$, alors $\alpha \in \mathbb{K}$.

• i/ $\Rightarrow$ iii/

Il est manifeste que le corps $\mathbb{K}$ est un sous-ensemble de $\mathbb{K}[\alpha]$. Si le réel α appartient au corps $\mathbb{K}$, les puissances successives de α, α^p appartiennent à $\mathbb{K}$, l'élément $x = \sum_{p=0}^{q} x_p \alpha^p$, $q \in \mathbb{N}$, $x_p \in \mathbb{K}$, appartient donc aussi à $\mathbb{K}$, par suite : $\mathbb{K}[\alpha] \subset \mathbb{K}$.

L'égalité $\mathbb{K}[\alpha]=\mathbb{K}$ a donc lieu.

• iii/ $\Rightarrow$ i/

L'égalité $\mathbb{K}[\alpha]=\mathbb{K}$, implique l'appartenance du réel α à $\mathbb{K}$.

I.3°. a. Par définition $\mathbb{K}[\alpha]$ est un sous-espace vectoriel de $\mathbb{K}$. Puisque α n'appartient pas à $\mathbb{K}$, la suite 1, α est libre dans le $\mathbb{K}$-espace vectoriel $\mathbb{K}[\alpha]$. Puisque le degré de α sur $\mathbb{K}$ est égal à 2, il existe des éléments a et b de $\mathbb{K}$ tels que :

$$\alpha^2 + a\,\alpha + b = 0\ ;\ a, b \in \mathbb{K}.$$

Les réels a et b vérifient la relation : $a^2 - 4\,b > 0$. Le réel α^2 et plus généralement tout réel α^k, $k \geq 2$, sont des combinaisons linéaires de 1 et de α. La suite 1, α est donc une base de $\mathbb{K}[\alpha]$. La dimension de $\mathbb{K}[\alpha]$ est donc égale à 2.

$\mathbb{K}[\alpha]$ est un anneau ; démontrons l'existence d'un inverse pour tout élément $x+y\alpha$ de $\mathbb{K}[\alpha]$:

$$(x+y\,\alpha)(u+v\,\alpha) = x\,u + (x\,v + y\,u)\alpha - y\,v\,(a\,\alpha + b)$$

$$(x+y\,\alpha)(u+v\,\alpha) = x\,u - y\,b\,v + \big((x - y\,a)v + y\,u\big)\alpha\,.$$

Le réel α n'appartient pas à $\mathbb{K}$; l'égalité $(x+y\,\alpha)(u+v\,\alpha) = 1$ est équivalente aux deux équations :

$$x\,u - y\,b\,v = 1,$$

$$y\,u + (x - y\,a)v = 0\,.$$

Le déterminant de ce système en u et v est :

$$\begin{vmatrix} x & \pm yb \\ y & x \pm ay \end{vmatrix} = x^2 - a\,x\,y + b\,y^2\ .$$

La forme quadratique $x^2 - a\,x\,y + b\,y^2$ n'est nulle que si x et y sont nuls car les éléments a et b de $\mathbb{K}$ vérifient la relation : $a^2 - 4\,b > 0$.

Remarque : il vient :

$$\begin{vmatrix} x & \pm yb \\ y & x \pm ay \end{vmatrix} = x^2 - a\,x\,y - (\alpha^2 + a\,\alpha)\,y^2 = (x - \alpha\,y)(x + \alpha y + ay)\,.$$

Le déterminant du système est différent de 0 car α et $\alpha + a$ n'appartiennent pas au corps $\mathbb{K}$. Il vient :

$$u = \frac{x - y\,a}{x^2 - a\,x\,y + b\,y^2},\quad v = -\frac{y}{x^2 - a\,x\,y + b\,y^2}\ .$$

Ces deux expressions sont des éléments du corps $\mathbb{K}$.

b . Remarquons que l'équation $X^2 + a\,X + b = 0$ admet des racines réelles ; par suite :

$$a^2 - 4b > 0.$$

Il vient : $\alpha = \frac{1}{2}\left(-a \pm \sqrt{a^2 - 4b}\right)$.

Posons : $k = a^2 - 4b$; k appartient à $\mathbb{K}$ mais $\sqrt{k}$ n'appartient pas à $\mathbb{K}$; car si $\sqrt{k}$ appartenait à $\mathbb{K}$, α appartiendrait aussi à $\mathbb{K}$.

- Puisque $\alpha = \frac{1}{2}(-a \pm \sqrt{k})$, le réel α appartient à $\mathbb{K}[\sqrt{k}]$; donc : $\mathbb{K}[\alpha] \subset \mathbb{K}[\sqrt{k}]$.

• d'un autre coté, il vient : $\sqrt{k} = \varepsilon(\alpha + \frac{a}{2})$; $\varepsilon = 1$ si $\alpha + \frac{a}{2} > 0$, -1 si $\alpha + \frac{a}{2} < 0$.

Par suite : $\mathbb{K}[\sqrt{k}\,] \subset \mathbb{K}[\alpha]$.

Les $\mathbb{K}$-espaces vectoriels engendrés par 1 et α d'une part 1 et $\sqrt{k}$ d'autre part sont donc égaux : $\mathbb{K}[\alpha] = \mathbb{K}[\sqrt{k}\,]$.

I-4° a. *Existence de* R : remarquons d'abord que, puisque le polynôme minimal de α est le polynôme M_α de degré n, tout réel α^k pour $k \geq n$ est une combinaison linéaire à coefficients dans $\mathbb{K}$ de réels α^k avec $k \leq n-1$. Par définition, un réel x appartenant à $\mathbb{K}[\alpha]$ s'écrit :

$$x = \sum_{k=0}^{r} x_k\, \alpha^k \text{ où r est un réel quelconque.}$$

Par suite tout réel x de $\mathbb{K}[\alpha]$ est une combinaison linéaire à coefficients dans $\mathbb{K}$ de réels α^k avec $k \leq n-1$. C'est-à-dire :

$$x = R(\alpha) .$$

Unicité de R : supposons que, pour un réel x de $\mathbb{K}[\alpha]$, il existe deux polynômes R_1 et R_2 appartenant à $\mathbb{K}_{n-1}[X]$ tels que :

$$x = R_1(\alpha) \text{ ; } x = R_2(\alpha) .$$

Il viendrait : $R_1(\alpha) - R_2(\alpha) = 0$.

Le polynôme $R_1 - R_2$ admettrait α comme racine alors qu'il est de degré $\leq n-1$. Ce qui est contraire à l'hypothèse : $d(\alpha, \mathbb{K}) = n$. Donc $R_1 - R_2 = 0$.

La suite $1, \alpha, \ldots, \alpha^{n-1}$ est donc libre et génératrice. Le $\mathbb{K}$-espace vectoriel $\mathbb{K}[\alpha]$ est de dimension n.

b. Le polynôme R a un degré $\leq n-1$; le polynôme M_α est irréductible dans $\mathbb{K}[X]$. Les polynômes M_α et R sont donc premiers entre eux. L'identité de Bézout prouve qu'il existe deux polynômes U et V appartenant à $\mathbb{K}[X]$ tels que :

$$U(x)\, R(x) + V(x)\, M_\alpha(x) = 1.$$

Il vient :

$$U(\alpha).R(\alpha) = 1.$$

c. L'ensemble $\mathbb{K}[\alpha]$ est un sous-ensemble du corps des réels. La seule propriété à vérifier est l'existence d'un inverse pour tout réel x différent de 0. Or :

$$\forall\, x \in \mathbb{K}[\alpha] ,\ x \neq 0, \exists\, R \in \mathbb{K}_{n-1}[X] \ : x = R(\alpha).$$

L'inverse de x est : $U(\alpha)$.

d . L'ensemble $\mathbb{K}[\alpha]$ est un corps. Le corps $\mathbb{K}[\alpha]$ contient $\mathbb{K}$ (donner à q la valeur 0 et à x_0 une valeur quelconque dans $\mathbb{K}$). Tout corps C, contenu dans $\mathbb{R}$, qui contient $\mathbb{K}$ et auquel le réel α appartient, contient toutes les puissances successives de α. Il contient par suite $\mathbb{K}[\alpha]$. $\mathbb{K}[\alpha]$ est donc le plus petit corps qui contient $\mathbb{K}$ et auquel le réel α appartient.

I-5°.a. Supposons que les polynômes P_n et P_{n+1} soient de degré respectivement égaux à n et n+1 et aient des coefficients entiers relatifs. Le polynôme P_{n+2} est alors de degré n+2 et ses coefficients sont des entiers relatifs.
Le coefficient du terme de plus haut degré de P_{n+1} est égal à 2-fois le coefficient du terme de plus haut degré de P_n. Par suite le coefficient de x^n de P_n est 2^n.
Il vient : $P_{n+2}(0) = - P_n(0)$.
Donc : $P_{2k}(0) = (-1)^k$; $P_{2k+1}(0) = (-1)^k$.

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

Manifestement : $Q_0(x) = 1$, $Q_1(x) = x + 1$,

$$\forall\, n \geq 0,\ Q_{n+2}(x) = x\, Q_{n+1}(x) - Q_n(x) ,$$

Par récurrence les coefficients des polynômes Q_n sont des entiers relatifs.

b . Désignons par $x = \frac{p}{q}$ une racine rationnelle du polynôme Q_n. Les entiers p et q sont premiers entre eux. Il vient :

$$p^n + p\, q\, (a_1\, p^{n-2} +\ldots+ a_k\, p^{n-k-1}\, q^{k-1} +\ldots+ a_{n-1}\, q^{n-2}) \pm q^n = 0 .$$

Cette relation prouve que l'entier p divise q^n ; or p est premier avec q ; p est donc égal à 1. Il vient :

$$1 + q\, (a_1 +\ldots+ a_k\, q^{k-1} +\ldots+ a_{n-1}\, q^{n-2} \pm q^{n-1}) = 0 .$$

L'entier q divise 1 donc q = 1.
Les seules racines rationnelles possibles du polynôme Q_n sont 1 et –1.

$$Q_{n+2}(x) = x\, Q_{n+1}(x) - Q_n(x) = x\,\big(x\, Q_n(x) - Q_{n-1}(x)\big) - Q_n(x).$$

$$Q_{n+2}(x) + x\, Q_{n-1}(x) = (x^2 - 1)\, Q_n(x) .$$

D'où :

$$Q_{n+3}(x) + x\, Q_n(x) = (x^2 - 1)\, Q_{n+1}(x) .$$

Si 1 (resp. –1) est racine de Q_n, 1 (resp. –1) est racine de Q_{n+3}.
Or :

$$Q_0(x) = 1\ ,\ \ Q_1(x) = x + 1\ ,\ Q_2(x) = x^2 + x - 1\ .$$

Les polynômes Q_{3k} n'ont pas de racines rationnelles.
Le réel -1 est la seule racine rationnelle des polynômes Q_{3k+1}.
Les polynômes Q_{3k+2} n'ont pas de racines rationnelles.

En conclusion : $-\frac{1}{2}$ est la seule racine rationnelle des polynômes P_{3k+1}, $k \geq 0$. Les autres polynômes n'ont pas de racines rationnelles.

I-6°. a. Il s'agit d'une suite récurrente linéaire ; recherchons son expression sous la forme d'une combinaison linéaire de deux suites géométriques ; l'équation caractéristique est :

$$r^2 - 2\, r \cos\theta - 1 = 0\ .$$

Les racines sont $e^{i\theta}$ et $e^{-i\theta}$. Par suite :

$$u_n = \lambda\, e^{in\theta} + \mu\, e^{-in\theta}\ .$$

Les deux scalaires λ et μ vérifient les relations :

- $\lambda + \mu = u_0$,
- $\lambda\, e^{i\theta} + \mu\, e^{-i\theta} = u_1$.

Par suite :

$$\boxed{u_n = -\, u_0\, \frac{\sin(n-1)\theta}{\sin\theta} + u_1\, \frac{\sin(n\theta)}{\sin\theta}}\ .$$

b . La suite des réels $v_n = P_n(\cos\theta)$ vérifie la relation de récurrence :

$$v_{n+2} = 2\, v_{n+1} \cos\theta - v_n\ .$$

et les conditions initiales :

$$v_0 = 1\ ;\ v_1 = 2\cos\theta + 1\ .$$

D'après le résultat précédent, il vient :

$$v_n = \lambda\, e^{in\theta} + \mu\, e^{-in\theta}\ .$$

- $\lambda + \mu = 1$,
- $\lambda\, e^{i\theta} + \mu\, e^{-i\theta} = 2\cos\theta + 1$.

Il vient :

$$\lambda = \frac{1 + e^{i\theta}}{2\, i\, \sin\theta}\ \ ;\ \ \mu = -\frac{1 + e^{-i\theta}}{2\, i\, \sin\theta}\ .$$

Donc :

$$P_n(\cos\theta) = \frac{1}{\sin\theta}(\sin(n+1)\theta + \sin n\theta) = \frac{1}{\sin\theta}\, 2\sin\left(\frac{2n+1}{2}\,\theta\right)\cos\left(\frac{\theta}{2}\right)\ .$$

Par suite : $$\boxed{P_n(\cos\theta) = \frac{\sin\left(\frac{(2n+1)\theta}{2}\right)}{\sin\frac{\theta}{2}}}$$

Le réel θ a été choisi strictement compris entre 0 et π ; il vient :

$$P_n(\cos\theta) = 0 \iff \sin\left(\frac{2n+1}{2}\theta\right) = 0 .$$

Or, pour $0 < \theta < \pi$:

$$\sin\left(\frac{2n+1}{2}\theta\right) = 0 \iff \theta = \frac{2k\pi}{2n+1}, \ 1 \leq k \leq n.$$

Le polynôme P_n est de degré n ; ses n racines distinctes sont donc les réels :

$$\boxed{x_{k,n} = \cos\left(\frac{2k\pi}{2n+1}\right),\ 1 \leq k \leq n.}$$

c . Donnons successivement à l'entier n les valeurs :

i/ n = 2 ; $\cos\left(\frac{2\pi}{5}\right)$ est racine du polynôme P_2 : $P_2(x) = 4x^2 + 2x - 1$.

ii/ n = 3 ; $\cos\left(\frac{2\pi}{7}\right)$ est racine du polynôme P_3 : $P_3(x) = 8x^3 + 4x^2 - 4x - 1$.

iii/ n= 4 : $\cos\left(\frac{2\pi}{9}\right)$ est racine du polynôme P_4 : $P_4(x) = 16x^4 + 8x^3 - 12x^2 - 4x + 1$.

Les polynômes P_2 et P_3 sont irréductibles sur $\mathbb{Q}$; par contre P_4 est divisible par $x+\frac{1}{2}$. Les polynômes minimaux sont respectivement :

$\frac{1}{4}(4x^2 + 2x - 1)$; $\frac{1}{8}(8x^3 + 4x^2 - 4x - 1)$; $\frac{1}{16}(16x^3 - 12x + 2)$.

C'est-à-dire :

$$x^2 + \frac{1}{2}x - \frac{1}{4} \ ; \qquad x^3 + \frac{1}{2}x^2 - \frac{1}{2}x - \frac{1}{8} \ ; \qquad x^3 - \frac{3}{4}x + \frac{1}{8} .$$

I-7°.a. D'après la question I-4°.a, l'espace vectoriel $\mathbb{Q}[\alpha]$ est de dimension trois puisque le polynôme minimal est de degré 3 : $x^3 - \frac{3}{4}x + \frac{1}{8}$.

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

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

b . Soit f un endomorphisme de $\mathbb{Q}[\alpha]$ tel que $f(x.y) = f(x).f(y)$.

• L'image de 1 par f vérifie :

$$f(1) = f(1)^2.$$

Puisque f est inversible la seule solution est $f(1) = 1$.

• Puisque le réel α vérifie la relation $\alpha^3 - \frac{3}{4}\alpha + \frac{1}{8} = 0$, l'image $f(\alpha)$ vérifie la relation :

$$f(\alpha)^3 - \frac{3}{4} f(\alpha) + \frac{1}{8} = 0 .$$

D'après la question précédente les valeurs possibles de $f(\alpha)$ sont :

$$f_1(\alpha) = \alpha \;\; ; \;\; f_2(\alpha) = 2\,\alpha^2 - 1 \;\; ; \;\; f_3(\alpha) = -2\,\alpha^2 - \alpha + 1 .$$

Les images de α^2 sont :

$$f_1(\alpha^2) = \alpha^2 \;\; ;$$

$$f_2(\alpha^2) = (2\,\alpha^2 - 1)^2 = -\alpha^2 - \frac{\alpha}{2} + 1 \;;$$

$$f_3(\alpha^2) = (-2\,\alpha^2 - \alpha + 1)^2 = \frac{\alpha}{2} + \frac{1}{2} .$$

Il n'y a donc que trois endomorphismes f vérifiant la relation $f(x.y) = f(x).f(y)$. L'endomorphisme composé de deux tels endomorphismes est encore un endomorphisme de ce type. Il s'agit d'un groupe à trois éléments.

Les matrices associées sont respectivement :

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} ; \begin{pmatrix} 1 & \pm 1 & 1 \\ 0 & 0 & \pm 1/2 \\ 0 & 2 & \pm 1 \end{pmatrix} ; \begin{pmatrix} 1 & 1 & 1/2 \\ 0 & \pm 1 & 1/2 \\ 0 & \pm 2 & 0 \end{pmatrix} .$$

I-8°.a. *Deux démonstrations* :

i/ L'expression S(r) s'écrit : $S(r) = \sum_{k=0}^{n} a_k\, r^k$. Les coefficients a_k, $0 \le k \le n$, sont des nombres rationnels. Par suite : $S(r) = \sum_{k=0}^{n} \frac{\alpha_k}{\beta_k} (\frac{p}{q})^k$.

Les entiers β_k, $0 \le k \le n$, sont strictement positifs. Soit M le P. G. C. D. des entiers $\beta_0, \beta_1, \ldots, \beta_p$; il vient :

$$S(r) = \frac{1}{M\, q^n} \sum_{k=0}^{n} \alpha_k \frac{M}{\beta_k}\, p^k\, q^{n \pm k} .$$

Chaque expression $\frac{M}{\beta_k}$ $0 \le k \le n$, est un entier ; l'expression $\sum_{k=0}^{n} \alpha_k \frac{M}{\beta_k}\, p^k\, q^{n \pm k}$ est par suite un entier relatif. Cet entier n'est pas nul car le polynôme S est supposé irréductible sur $\mathbb{Q}$. Sa valeur absolue est supérieure ou égale à 1. Donc :

$$|S(r)| \geq \frac{1}{C_S\, q^n} \quad ;\text{ en posant : } C_S = M\ (\text{P. G. C. D. des } \beta_k,\ 0 \leq k \leq n).$$

ii/ Puisque le polynôme S a des coefficients rationnels, il existe un plus petit entier C_S strictement positif tel que le polynôme Π défini par la relation

$$\Pi(x) = C_S\ S(x) = \sum_{k=0}^{n} a_k\, x^k\ ,$$

ait des coefficients a_k, $0 \leq k \leq n$, entiers relatifs. Par suite :

$$\Pi(r) = \frac{1}{q^n} \sum_{k=0}^{n} a_k\, p^k\, q^{n \pm k}.$$

Puisque le polynôme S est irréductible sur $\mathbb{Q}$, le réel r n'est racine ni de S ni de Π. La valeur absolue de l'entier relatif $\sum_{k=0}^{n} a_k\, p^k\, q^{n \pm k}$ est supérieure ou égale à 1

Donc :

$$\boxed{|S(r)| \geq \frac{1}{C_S\, q^n}}$$

b . Appliquons la formule des accroissements finis :

$$S(r) - S(\alpha) = (r - \alpha)\, S'(\alpha + \theta\, r\,);$$

Il vient : $|S(r)| \leq |r - \alpha| \sup\limits_{\alpha \pm 1 \leq x \leq \alpha + 1} |S'(x)|$;

La fonction $x \mapsto |S'(x)|$ est bornée sur l'intervalle $[\alpha - 1,\ \alpha + 1]$. Soit M son maximum. Par suite :

$$|S(r)| \leq M\, |r - \alpha|\ .$$

Donc :

$$\boxed{|r - \alpha| \geq \frac{1}{M\, C_S\, q^n} = \frac{K}{q^n}}$$

c . • *Deux démonstrations* :

i/ Démontrons que la suite t_n, $n \geq 0$, est une suite de Cauchy ; soient $p \geq q \geq n$:

$$t_p - t_q = \sum_{k=q+1}^{p} 10^{\pm k!} \leq \sum_{k=q+1}^{p} 10^{\pm k} \leq \frac{1}{10^n}\,\frac{10}{9}\ .$$

ii/ A cause de l'inégalité, $10^{-n!} \leq 10^{-n}$, la série de terme général t_n, $n \geq 0$, est convergente.

• Soit t la limite de la suite t_n, $n \geq 0$:

$$t - t_n = \sum_{k=n+1}^{\infty} 10^{\pm k!} \leq 10^{-(n+1)!} \sum_{k=0}^{\infty} 10^{\pm k} = \frac{10}{9}\, 10^{-(n+1)!} \leq 2\times 10^{-(n+1)!}.$$

• Si le réel t était rationnel ou algébrique sur $\mathbb{Q}$, il serait racine d'un polynôme P de degré 1 ou supérieur strictement à 1 appartenant à $\mathbb{Q}[X]$. D'après la question précédente, il existerait une constante K telle que pour tout rationnel r de l'intervalle $[t-1, t+1]$ l'inégalité $|t - r| \geq \dfrac{K}{q^n}$ aurait lieu.

Appliquons cette inégalité aux réels t_p, $p \geq 0$; il viendrait : $|t - t_p| \geq \dfrac{K}{10^{p!}}$.

Or : $|t - t_p| \leq 2\times 10^{-(p+1)!}$.

La constante K vérifierait l'inégalité : $K \leq 2\times 10^{-(p+1)}$. Ce qui est contraire au fait que la contante K est strictement positive.

Seconde partie.

II-1°. • Soient A (a, b) et A′(a′, b′) deux points de $\mathbb{K}$. Une équation de la droite passant par A et A′ est :

$$\frac{x - a}{a - a'} = \frac{y - b}{b - b'} \; .$$

Les coefficients de cette équation sont, comme a, b, a′, b′, dans $\mathbb{K}$.

La distance des deux points A et A′ est :

$$d = \sqrt{(a - a')^2 + (b - b')^2} \; .$$

Une équation du cercle de centre C (c, d) et de rayon R égal à la distance de A au point A′ est :

$$(x - c)^2 + (y - d)^2 = (a - a')^2 + (b - b')^2 \; .$$

Les coefficients de cette équation sont dans $\mathbb{K}$.

• Les solutions d'un système de Cramer à coefficients dans $\mathbb{K}$ sont encore dans $\mathbb{K}$. Les deux droites ont des équations à coefficients dans $\mathbb{K}$. La solution, supposée exister, des équations est un couple de réels appartenant à $\mathbb{K}$.

• Supposons la droite et le cercle donnés par des équations à coefficients dans $\mathbb{K}$:

$$ax + by = c,\; (x - c)^2 + (y - d)^2 = e \; .$$

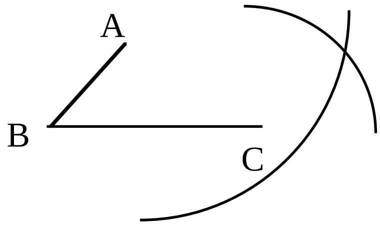
L'équation aux abscisses est une équation du second degré dont les coefficients sont dans $\mathbb{K}$. Si cette équation admet une racine double, cette racine est dans $\mathbb{K}$. Si les solutions sont distinctes, elles sont dans une extension quadratique de $\mathbb{K}$.

• Un point commun à deux cercles de $\mathfrak{C}$ est aussi un point d'intersection de l'un des deux cercles et de l'axe radical. C'est donc un point situé à l'intersection d'une droite et d'un cercle à coefficients dans $\mathbb{K}$.

II-2°.a.

• *Deux méthodes* :

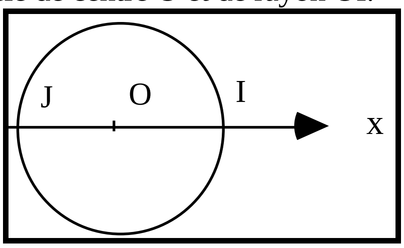
i/ Le point D est situé à l'intersection des deux cercles centrés en A et C et de rayons respectivement égaux aux longueurs des cotés BC et AB.



ii/ On construit, à la règle et au compas, la médiatrice du segment [AC]. Le point d'intersection de cette médiatrice avec [AC] donne le milieu I de [AC]. Le symétrique D de B par rapport à I s'obtient comme intersection de la droite AI et du cercle de centre I et de rayon IB.

• La parallèle à la droite Δ passant par le point A s'obtient en construisant un parallèlogramme dont les trois premiers sommets sont A et deux points B et C situés sur Δ.

b. • Le point J est constructible comme intersection de la droite (Ox), joignant les points O et I, et du cercle de centre O et de rayon OI.

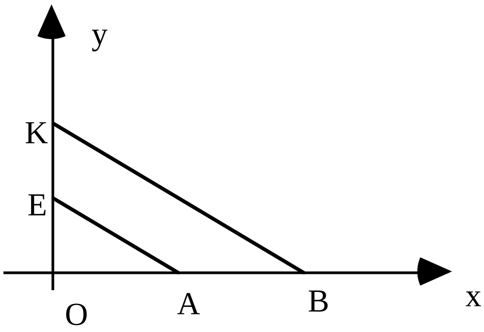


L'axe Oy se construit comme médiatrice du segment IJ. Le point K est à l'intersection de cette médiatrice et du cercle de centre O de rayon OI.

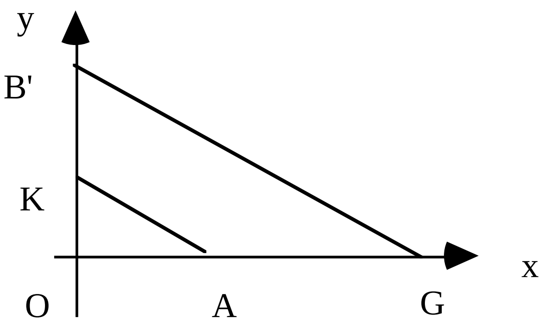
• Soient A et B les deux points de l'axe Ox d'abscisses respectivement égales à α et β.

i/ Le point C d'abscisse $\alpha + \beta$ est l'intersection de la droite OB avec le cercle de centre B de rayon OA.

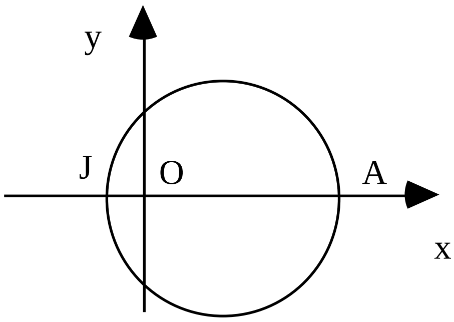
ii/ Utilisons le théorème de Thalès : soit E le point d'intersection avec l'axe Oy de la parallèle à la droite BK menée par A : l'ordonnée de E est égale à $\frac{\alpha}{\beta}$.



Soit B' le point de Oy d'ordonnée β. L'ordonnée du point G intersection de l'axe Ox et de la parallèle à la droite AK passant par B' est égale à $\alpha.\beta$



• Le centre ω du segment joignant J $(-1, 0)$ au point A $(\alpha, 0)$ est constructible (médiatrice du segment [JA]) ; considérons le cercle de centre ω et de rayon ωA ; il coupe l'axe Oy en deux points d'ordonnées $\pm\sqrt{\alpha}$.



II-3°. a. Si un point M du plan P est constructible, c'est un point construit à partir d'un ensemble de points$\{O, I, M_1, M_2, \ldots, M_{j-1}\}$. Les coordonnées du point M_1 sont des racines de polynômes de coefficients rationnels ; elles appartiennent à $\mathbb{Q}$ ou à un corps $\mathbb{K}_1$. De même, si les coordonnées de M_j appartiennent au corps $\mathbb{K}_i$, les coordonnées du point M_{j+1} appartiennent au corps $\mathbb{K}_i$ ou à une de ses extensions quadratiques $\mathbb{K}_{i+1}$. D'où le résultat.

b . Tous les points dont les coordonnées sont des entiers relatifs sont constructibles (II-2°.b).

Les points de coordonnées rationnelles sont constructibles (II-2°.b).

Étant donné un corps $\mathbb{K}_i$, supposons tous les points dont les coordonnées sont dans $\mathbb{K}_i$, constructibles. Les points d'intersection de droites ou de cercles appartenant aux ensembles $\mathfrak{D}$ ou $\mathfrak{C}$, appartiennent au corps $\mathbb{K}_i$ ou à une de ses extensions quadratiques. Ils appartiennent donc à un corps $\mathbb{K}_{i+1}$.

II-4°.a Puisque G est un F-espace vectoriel de dimension q, il existe une base constituée des éléments : $\gamma_1, \gamma_2,\ldots,\gamma_q$. Tout élément g de G s'écrit de manière unique au moyen de scalaires f_i, $1\le i\le q$, dans F :

$$g = \sum_{i=1}^{q} f_i\, \gamma_i\,.$$

Puisque H est un G-epace vectoriel de dimension r, il existe une base constituée des éléments : $\eta_1, \eta_2,\ldots,\eta_r$. Tout élément h de H s'écrit de manière unique au moyen de scalaires g_i, $1\le i\le r$, dans G :

$$h = \sum_{i=1}^{r} g_i\, \eta_i\,.$$

En particulier chaque scalaire g_i s'écrit dans la base de G, $\gamma_1, \gamma_2,\ldots,\gamma_q$. :

$$g_j = \sum_{k=1}^{q} f_{j,k}\, \gamma_k\,.$$

Il vient par suite : $$h = \sum_{i,k} f_{i,k}\, \gamma_k\, \eta_i\,.$$

Les éléments $\gamma_k.\eta_i$, $1\le k\le q$, $1\le i\le r$, appartiennent à l'espace vectoriel H ; en considérant H comme un F-espace vectoriel, cette famille est génératrice. Démontrons que la suite $(\gamma_k\, \eta_i)_{k,i}$ est indépendante. Soient $m_{i,k}$ des scalaires appartenant à F tels que :

$$\sum_{i,k} m_{i,k}\, \gamma_k\, \eta_i = 0.$$

C'est-à-dire : $$\sum_{i=1}^{r} \eta_i \sum_{k=1}^{q} m_{i,k}\, \gamma_k = 0\,.$$

Puisque la suite η_i est une base du G-espace vectoriel H, il vient :

$$\sum_{k=1}^{q} m_{i,k}\, \gamma_k = 0\,.$$

Puisque la suite γ_i est une base du F-espace vectoriel G, il vient :

$$\forall\ i,k\ ,\ m_{i,k} = 0.$$

La dimension du F-espace vectoriel G est donc égal au produit qr.

b . Une extension quadratique d'un corps $\mathbb{K}$ est un $\mathbb{K}$-espace vectoriel de dimension 2. Par suite le $\mathbb{Q}$-espace vectoriel $\mathbb{K}_n$ est de dimension 2^n.

c . D'après la question II-3°.a, si le réel α est constructible, il appartient à un corps $\mathbb{K}_i$ appartenant à une suite finie de corps ayant la propriété ($\mathfrak{P}$). Or ce corps est un $\mathbb{Q}$-espace vectoriel de dimension 2^i. Par suite le degré de α est 2^i.

II-5°. Pour que le polygone régulier à n côtés soit constructible, il faut et il suffit que le réel $\cos(\frac{2\pi}{n})$ soit constructible. Utilisons les résultats précédents :

n	$\alpha = \cos(\frac{2\pi}{n})$	$d(\alpha,\mathbb{Q})$	$\alpha \in 2^{\mathbb{N}}$?	constructibilité ?
3	$-1/2$	1	oui	oui
4	0	1	oui	oui
5	$(\sqrt{5}-1)/4$	2	oui	oui
6	$1/2$	1	oui	oui
7	$P_3(\alpha) = 0$	3	non	non
8	$\sqrt{2}/2$	2	oui	oui
9	$P_4(\alpha) = 0$	3	non	non
10	$(\sqrt{5}+1)/4$	2	oui	oui

<u>Remarque</u> : Le réel α appartient à $\mathbb{Q}$ pour n = 3, 4 et 6, à une extension quadratique de $\mathbb{Q}$ pour n = 5, 8 et 10 ; en dehors de ces cas le réel α n'appartient ni à $\mathbb{Q}$ ni à une extension quadratique de $\mathbb{Q}$.

FIN