Nombres algébriques, nombres transcendants, constructions à la règle et au compas.

Partie I : Généralités et exemples.

1°) C'était du cours avant 2004.
2°) Évident.
3°) a) Théorème du cours (avant 2004) : $\dim_K(K[\alpha]) = \deg(M_\alpha)$.
b) α est racine *réelle* d'une équation algébrique de degré 2 de la forme $\alpha^2 - s\alpha + p = 0$, s et p étant éléments de K, donc réels. Dans ces conditions, α s'exprime dans $\mathbb{R}$ par la formule $\alpha = \dfrac{s \pm \sqrt{k}}{2}$, avec $k = s^2 - 4p \in K_+$. Ceci nous pousse à examiner $\delta = 2\alpha - s \in K[\alpha]$; on a $\delta^2 = 4\alpha^2 - 4s\alpha + s^2 = s^2 - 4p = k$, soit bien $\delta = \sqrt{k}$. En conséquence, on a $\sqrt{k} \subset K[\alpha]$, donc $K[\sqrt{k}] \subset K[\alpha]$ par le principe du sous-corps engendré ; d'autre part, on a évidemment $\alpha \in K[\sqrt{k}]$, d'où l'égalité par le même principe. Dans le vocabulaire de la théorie de Galois, on peut dire que : $\boxed{\text{Toute extension quadratique réelle est une extension radicale.}}$

Remarque : La restriction de α à être réel n'est pas fondamentale, et a été placée tout au long du problème pour simplifier les raisonnements en évitant d'avoir à choisir les "bonnes" racines.
4°) La base de $K[\alpha]$ est $(1, \alpha, \dots, \alpha^{n-1})$: c'est désormais du cours. Les autres énoncés sont aussi des conséquences du théorème du cours.
5°) Polynômes de Tchebycheff modifiés.
a) Les polynômes Q_n vérifient la relation de récurrence $Q_{n+1} = XQ_n - Q_{n-1}$, avec $Q_0 = 1$ et $Q_1 = X + 1$. Par rapport aux polynômes de Tchebycheff classiques, introduits dans le cours, tels que $T_0 = 2, T_1 = X, U_0 = 1, U_1 = X$, on a ici tout bonnement $U_n + U_{n-1}$. Ceci servira à la question 6. En attendant, des récurrences immédiates montrent que $\deg Q_n = n$, $Q_n \in \mathbb{Z}[X]$, Q_n unitaire, $Q_n(0) = 1$ si $n \equiv 0$ ou $n \equiv 1 \bmod 4$, $Q_n(0) = -1$ sinon ; soit $Q_n(0) = (-1)^{\frac{n(n-1)}{2}}$. On en déduit que $\deg P_n = n$, P_n a pour coefficient dominant 2^n et $P_n(0) = (-1)^{\frac{n(n-1)}{2}}$.
b) Une racine rationnelle $\dfrac{a}{b}$ d'un polynôme à coefficients entiers $P = \sum_{i=0}^{n} a_i X^i$ doit avoir son numérateur a qui divise le coefficient constant a_0 et son dénominateur b qui divise le coefficient dominant. Ici, on a $a = \pm 1$ et $b = \pm 1$.
La relation de récurrence qui définit les Q_n montre que
$$Q_{n+3} + XQ_n = XQ_{n+2} - Q_{n+1} + XQ_n = X^2 Q_{n+1} - XQ_n - Q_{n+1} + XQ_n = (X^2 - 1)Q_{n+1}\,.$$
Dès lors, Q_n et Q_{n+3} ont les mêmes racines parmi 1 et -1.
D'autre part, on a $Q_0 = 1, Q_1 = X + 1, Q_2 = X^2 + X - 1$. Seul Q_1 a une racine rationnelle qui est -1 ; donc seuls les Q_{3k+1} ont une racine rationnelle, qui vaut -1. Dès lors, seuls les P_{3k+1} ont une racine rationnelle, qui est $-\dfrac{1}{2}$.
6°) a) Il faudrait appliquer le principe des suites récurrentes linéaires (à la recherche de suites géométrique solutions, poser une équation du second degré, la résoudre dans $\mathbb{C}$, examiner les premiers termes et conclure). Nous détournons cette question ci-dessous.
b) On a noté ci-dessus que $Q_n = U_n + U_{n-1}$; donc
$$Q_n(2\cos\theta) = \frac{\sin n\theta + \sin(n+1)\theta}{\sin\theta} = \frac{2\sin(2n+1)\frac{\theta}{2}\cos\frac{\theta}{2}}{2\sin\frac{\theta}{2}\cos\frac{\theta}{2}} = \frac{\sin(2n+1)\frac{\theta}{2}}{\sin\frac{\theta}{2}}$$
d'où il résulte que $P_n(\cos\theta) = \dfrac{\sin(2n+1)\frac{\theta}{2}}{\sin\frac{\theta}{2}}$. Ce polynôme s'annule pour $\theta \in]0, \pi[$ lorsque $\sin(2n+1)\frac{\theta}{2} = 0$, soit $\theta = \dfrac{2k\pi}{2n+1}$ (pour n valeurs de k : $1 \leqslant k \leqslant n$) ce qui donne n racines réelles distinctes de P_n qui sont $\boxed{x_{k,n} = \cos\dfrac{2k\pi}{2n+1} \text{ avec } 1 \leqslant k \leqslant n.}$

c) Le nombre $\cos\dfrac{2\pi}{5}$ est donc racine de $P_2 = 4X^2 + 2X - 1$ donc algébrique sur $\mathbb{Q}$ et de degré 2 car non rationnel (voir question 5b). Ainsi, P_2 est polynôme minimal de $\cos\dfrac{2\pi}{5}$.
Le nombre $\cos\dfrac{2\pi}{7}$ est racine de $P_3 = 8X^3 + 4X^2 - 4X - 1$ donc algébrique sur $\mathbb{Q}$ et de degré 3 au plus. Enfin, P_3 n'a pas de racine rationnelle (question 5b), donc ne peut aucunement se factoriser sur $\mathbb{Q}$; il est irréductible et est le polynôme minimal de $\cos\dfrac{2\pi}{7}$ qui est finalement de degré 3.
Le nombre $\cos\dfrac{2\pi}{9}$ est racine de P_4 donc algébrique sur $\mathbb{Q}$ et de degré 4 au plus. Mais, P_4 a une racine rationnelle (question 5b), et va se factoriser en produit d'un polynôme de degré 3 et d'un polynôme de degré 1. Explicitement, on a $Q_4 + X(X+1) = (X^2 - 1)Q_2 = (X^2 - 1)(X^2 + X - 1)$ soit $Q_4 = (X+1)(X^3 - 3X + 1)$. Le polynôme $X^3 - 3X + 1$ ne peut avoir comme éventuelles racines rationnelles que 1 ou -1, et il n'en admet aucune en fait ; il est donc irréductible sur $\mathbb{Q}$; par conséquent, le polynôme minimal de $\cos\dfrac{2\pi}{9}$ sera $\dfrac{P_4}{2X+1} = N = 8X^3 - 6X + 1$, et le degré de ce nombre algébrique est bien 3.
Remarque : historiquement, les Grecs d'Alexandrie, dont Euclide, furent très préoccupés de la difficulté apparente de construire certains objets géométriques à la règle et au compas. Faute de trouver des solutions explicites et de pouvoir démontrer les impossibilités qu'on verra au II (deux millénaires plus tard !), ils imaginèrent de faire appel à des tracés nouveaux, comme la Cissoïde de Dioclès ou la Conchoïde de Nicomède. Ces courbes leur permirent de réaliser la "trissection" de l'angle, donc de "construire" l'ennéagone (9 côtés), ou de "dupliquer le cube". De telles idées furent incorporées bien plus tard, par Abel, dans le cadre de la Théorie des Groupes et de la Géométrie Algébrique.

$\mathbb{Q}$. On calcule aisément les trois racines non rationnelles de P_4, donc de $8X^3-6X+1$, ce sont $\alpha=\cos\dfrac{2\pi}{9}$, $\beta=2\alpha^2-1=\cos\dfrac{4\pi}{9}$ et $\gamma=-\alpha-2\alpha^2+1=\cos\dfrac{8\pi}{9}$, car la somme des racines de $N=8X^3-6X+1$ est nulle.

b) La multiplicativité de f montre que $f(1)=f(1)^2$; si $f(1)=0$, alors $f(x)=f(x.1)=f(x)f(1)=0$; l'auteur du sujet a oublié l'application nulle ! Sinon, on a $f(1)=1$ et f est un endomorphisme de corps ; il est donc injectif et même bijectif par $\mathbb{Q}$-linéarité.

Le caractère morphique de f fait que la relation $8\alpha^3-6\alpha+1=0$ se transfère à $f(\alpha)$; en somme, f permute les racines de $8X^3-6X+1$. Il y a a priori six permutations possibles, mais on va voir que seules les permutations paires conviennent. En effet, si on avait (par exemple) $f(\alpha)=\alpha$, alors $f(\alpha^2)=f(\alpha)^2=\alpha^2$ donc par linéarité f est l'application identité sur $\mathbb{Q}[\alpha]$. Pareillement, si $f(\alpha^2)=\alpha^2$ alors $f(\alpha^4)=\alpha^4$; or, $8\alpha^4=6\alpha^2-\alpha$, donc $f(\alpha)=\alpha$. Ainsi, f fixe les trois racines du polynôme minimal, ou n'en fixe aucune. Il ne reste que deux possibilités non triviales (et mutuellement réciproques) : $\alpha\to\beta\to\gamma$ et $\alpha\to\gamma\to\beta$.

L'étude précédente laisse de côté le problème de l'existence de ces endomorphismes. Définissons d'abord f tel que $f(\alpha)=\beta$. Il est nécessaire que $f(\alpha^2)=\beta^2$. Réciproquement, la formule $f(x+y\alpha+z\alpha^2)=x+y\beta+z\beta^2$ définit-elle un morphisme d'anneaux ? Pour ce vérifier, il suffit de le tester sur les éléments de la base (à cause de la linéarité). Le calcul revient à vérifier que $f(\alpha^p)=f(\beta^p)$. On divise X^p par N : $X^p=NQ+R$, le reste étant de degré 2 au plus : $R=uX^2+vX+w$. On a donc $\alpha^p=N(\alpha)Q(\alpha)+u\alpha^2+v\alpha+w=u\alpha^2+v\alpha+w$ et aussi $\beta^p=N(\beta)Q(\beta)+u\beta^2+v\beta+w=u\beta^2+v\beta+w$. Dès lors, on a $f(\alpha^p)=uf(\alpha^2)+vf(\alpha)+w=u\beta^2+v\beta+w=\beta^p$. En conclusion,

$$\boxed{\begin{array}{l}\text{il y a trois automorphismes du corps } \mathbb{Q}[\alpha], \text{ définis par}\\ \text{les trois permutations paires des racines du polynôme minimal de } \alpha.\end{array}}$$

Les matrices se calculent aisément ; par exemple, f telle que $f(\alpha)=\beta=2\alpha^2-1$ vérifie $f(\alpha^2)=(2\alpha^2-1)^2=4\alpha^4-4\alpha^2+1=(8\alpha^3-6\alpha+1)\dfrac{\alpha}{2}-\alpha^2-\dfrac{\alpha}{2}+1$ (à vérifier) et a pour matrice $\begin{pmatrix}1&-1&1\\0&0&-\frac12\\0&2&-1\end{pmatrix}$. L'autre automorphisme non identique a une matrice inverse de celle-ci.

8°) Approximations rationnelles d'un nombre algébrique réel selon Liouville.

a) Soit $S(x)=s_nx^n+\cdots+s_0$ avec $s_n\neq 0$ et les s_k dans $\mathbb{Q}$, irréductible sur $\mathbb{Q}$. Quitte à multiplier S par le ppcm des dénominateurs des s_i, que nous noterons C_S, on peut remplacer S par une polynôme S_0 proportionnel et à coefficients entiers. Comme S_0 est irréductible, il n'a pas de racine rationnelle. On a donc $S_0(\dfrac{p}{q})=\dfrac{N}{q^n}\neq 0$, N étant un certain entier non nul. Par conséquent, $|S_0(\dfrac{p}{q})|\geqslant\dfrac{1}{q^n}$ et donc $|S(\dfrac{p}{q})|\geqslant\dfrac{1}{C_Sq^n}$.

b) Soit α algébrique de degré $n\geqslant 2$, zéro de S.

Considérons à présent la restriction de S à l'intervalle $[\alpha-1,\alpha+1]$; sa dérivée y reste bornée, donc on grâce au théorème des Accroissements Finis une condition de Lipschitz pour S qui s'écrit $|S(x)-S(y)|\leqslant M|x-y|$. Considérons ensuite une approximation $\frac{p}{q}$ de α, telle que $\frac{p}{q}\in[\alpha-1,\alpha+1]$ (pour q assez grand c'est possible). On a $|S(\dfrac{p}{q})|\geqslant\dfrac{1}{C_Sq^n}$ et donc $M|\alpha-\dfrac{p}{q}|\geqslant|S(\dfrac{p}{q})-S(\alpha)|\geqslant\dfrac{1}{C_Sq^n}$, soit $|\alpha-\dfrac{p}{q}|\geqslant\dfrac{K}{q^n}$, avec $K=\dfrac{1}{MC_S}$.

c) Une inégalité $\dfrac{C}{q^{n+1}}\geqslant\dfrac{K}{q^n}$ ne peut avoir lieu pour une infinité d'entiers q. On a alors la conséquence suivante : Pour prouver qu'un réel non rationnel t est transcendant, il suffit de vérifier que, pour tout $n\geqslant 1$, il existe une infinité de rationnels $\frac{p}{q}$ avec $q>0$ et (p,q) premiers entre eux, tels que l'on ait $|t-\dfrac{p}{q}|\leqslant\dfrac{1}{q^{n+1}}$.

Étant donné un entier $p\geqslant 2$, on appelle nombre de Liouville tout réel somme d'une série de terme général $\frac{a_n}{p^{n!}}$ avec les a_n entiers compris entre 0 et $p-1$, non tous nuls à partir d'un certain rang. Une telle série converge aisément (majorer par une série géométrique). On va prouver que tout nombre de Liouville est transcendant.

Soit un nombre de Liouville $t=\sum\limits_{n=0}^{\infty}\dfrac{a_n}{p^{n!}}$. En posant $s_n=\sum\limits_{k=0}^{n}\dfrac{a_k}{p^{k!}}$, on a

$$|t-s_n|=\sum_{k=n+1}^{\infty}\frac{a_k}{p^{k!}}\leqslant(p-1)\sum_{k=n+1}^{\infty}\frac{1}{p^{k!}}=\frac{p-1}{p^{(n+1)!}}\sum_{k=n+1}^{\infty}\frac{1}{p^{k!-(n+1)!}}\leqslant\frac{p-1}{p^{(n+1)!}}\sum_{k=n+1}^{\infty}\frac{1}{p^{k-n-1}}=\frac{1}{p^{(n+1)!-1}}$$

et par suite t est transcendant.

Partie II : Constructions à la règle et au compas

1°) *Droite de $\mathcal{D}$:* on a l'équation $(x-x_1)(y_2-y_1)=(y-y_1)(x_2-x_1)$ qui a ses coefficients dans K.

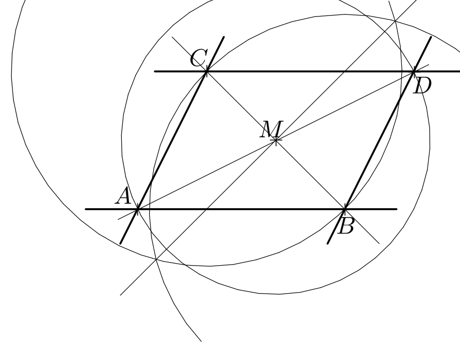
Cercle de $\mathcal{C}$: on a l'équation $(x-x_0)^2+(y-y_0)^2=(x_1-x_2)^2+(y_1-y_2)^2$ qui a ses coefficients dans K.

Intersection de droites de $\mathcal{D}$: un système linéaire a ses solutions qui répondent aux formules de Cramer, qui sont rationnelles par rapport aux coefficients, donc restent dans K.

Intersection de droite et de cercle : on confronte $x^2+y^2-2ax-2by+c=0$ $(a,b,c\in K)$ avec $y=mx+p$ $(m,p\in K)$. On en tire une équation du second degré $x^2+(mx+p)^2-2ax-2b(mx+p)+c=0$, dont les deux solutions appartiennent à une extension quadratique de K, selon la question I3. Il se peut qu'il n'y ait qu'une racine (double : cercle et droite tangents) ; alors le discriminant est nul et la racine reste dans K. L'abscisse ayant été "calculée", l'ordonnée s'en déduit par $y=mx+p$, ce qui reste dans K ou dans l'extension quadratique dont on vient de parler.

Intersection de cercles : on confronte $x^2+y^2-2ax-2by+c=0$ $(a,b,c\in K)$ avec $x^2+y^2-2a'x-2b'y+c'=0$ $(a',b',c'\in K)$. Cela revient à $x^2+y^2-2ax-2by+c=0=2(a-a')x+2(b-b')y-(c-c')$, et on est ramenés au cas précédent (en fait, on trace l'axe radical des deux cercles). Donc les deux points d'intersection ont des coordonnées dans une extension quadratique de K ou dans K si les deux cercles sont tangents.

2°) a) On construit le quatrième sommet du parallélogramme de la manière suivante (ce n'est pas la seule, mais elle a l'avantage de rester valide lorsque les points sont alignés) : on trace le cercle de centre C et de rayon BC ; puis le cercle de centre B et de même rayon ; ils se coupent en deux points M, P ; on trace la droite (MP) et la droite (BC) qui se coupent au milieu Q du segment $[B, C]$ (et centre du parallélogramme). On trace la droite (AQ) et le cercle de centre Q, rayon AQ. Cette droite et ce cercle se coupent en A et en D que l'on cherche.
Si A et Δ sont tracés, c'est que sur Δ il y a deux points B et C déjà tracés. On construit le parallélogramme $ABCD$, de sorte que la droite (AD) est la parallèle cherchée.



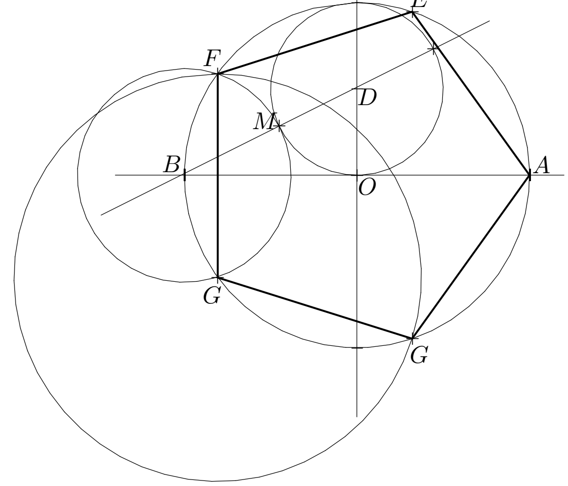
b) On obtient J par l'intersection de (OI) et du cercle de centre O passant par I. Les cercles de centres I et J et de même rayon IJ se coupent en deux point F, G ; la droite (FG) est l'axe des ordonnées et coupe le tout premier cercle en K et L.
Pour construire la somme de deux nombres réels constructibles, il suffit d'appliquer la méthode vue ci-dessus au parallélogramme (aplati) formé par les points d'abscisses $0, \alpha, \beta$ et $\alpha + \beta$, et ordonnées nulles. Pour construire produits, inverses, racines, on va placer des cercles passant par trois points déjà tracés (on sait construire : le centre provient de l'intersection de deux médiatrices), et intersecter ces cercles avec l'un des axes. A cet effet, nous servira le

Lemme. *Si un cercle du plan complexe coupe l'axe réel en des points d'affixes a, b et l'axe imaginaire pur en des points d'affixes ic, id, alors on a $ab = cd$.*

Le cercle a une équation qu'on peut écrire $x^2 + y^2 - 2ux - 2vy + w = 0$. L'intersection avec l'axe Ox amène l'équation $x^2 - 2ux + w = 0$, donc $w = ab$. L'intersection avec l'axe Oy amène l'équation $y^2 - 2vy + w = 0$, donc $w = cd$, ce qu'il fallait !
Produits : considérer le cercle passant par les points $A = (\alpha, 0); B = (\beta, 0); K = (0, 1)$. Il recoupe l'axe des ordonnées en un point de coordonnées $(0, c)$; d'après le Lemme on a $\alpha\beta = 1 \times c$. Il suffit de ramener ce point sur l'axe des abscisses par un cercle de centre O et le tour est joué.
Inverses : considérer le cercle passant par les points de coordonnées $A = (\alpha, 0); K = (0, 1); L = (0, -1)$. Il recoupe l'axe des abscisses en un point de coordonnées $(c, 0)$; d'après le Lemme on a $\alpha c = 1 \times (-1) = -1$. Il suffit de faire subir au point $(c, 0)$ un demi-tour de centre O pour obtenir $(\dfrac{1}{a}, 0)$.
Quotients : combinaison des deux méthodes précédentes.
Racines : considérer le cercle de diamètre AJ, passant par les points de coordonnées $A = (\alpha, 0); J = (-1, 0); M = (0, c); N = (0, -c)$; d'après le Lemme on a $\alpha \times (-1) = c \times (-c)$ soit $c = \sqrt{\alpha}$. Il suffit de ramener le point $(0, c)$ sur l'axe des abscisses par un cercle de centre O et la construction est achevée.
3°) a) Si M est un point constructible, il est atteint à la suite de la construction de points intermédiaires M_i.
On passe de M_0 et M_1 à M_2 en appliquant l'une des règles prescrites, c'est-à-dire en traçant la droite qui les joint, et un ou deux cercles de centre M_0 ou M_1, puis en intersectant la droite et un cercle, ou les deux cercles. Il résulte par la question 1 que les coordonnées de M_2 sont dans K_2, extension quadratique de $K_1 = \mathbb{Q}$.
Supposons que les points $M_2, \ldots, M_i$ aient leurs coordonnées dans un corps K_i. Le prochain point peut réclamer le tracé de droites joignant certains des M_j déjà trouvés, et les coefficients de leurs équations restent dans K_i ; il peut aussi réclamer le tracé de cercles centrés sur certains des M_j et ayant un rayon égal à la distance de deux des M_i. Les coefficients des équations de ces cercles restent encore dans K_i (question 1 toujours). Donc tous les éléments “intermédiaires” de la construction restent dans K_i. Le passage final est une intersection, qui peut se faire “dans K_i”, ou sinon réclamer le passage à une extension quadratique K_{i+1} de K_i. Dans le premier cas, on pose tout simplement $K_{i+1} = K_i$.
La récurrence fonctionne donc et prouve que tout point constructible a ses coordonnées dans le “sommet” d'une “pile d'extensions quadratiques” de $\mathbb{Q}$.
b) Soit une pile (K_i) d'extensions quadratiques. Les éléments du premier sont constructibles : il s'agit des nombres rationnels, constructibles comme quotients d'entiers selon II2b. Supposons que les éléments de K_i soient tous constructibles. Ceux de $K_{i+1} = K_i[\sqrt{k_i}]$ peuvent s'écrire sous la forme $x + y\sqrt{k_i}$, x, y, k_i étant dans K_i. On construit $\sqrt{k_i}$ comme indiqué au II2b, puis le produit $y\sqrt{k_i}$ de même, enfin la somme suivant le procédé prévu. En conséquence, tout élément de K_{i+1} est constructible.
4°) a) On suppose que G est une extension de dimension finie sur F et que H est une extension de dimension finie sur G. Montrons que H est une extension de dimension finie sur F.
On considère une base (x_i) de G sur F et une base (y_j) de H sur G, avec $\dim_F G = q$ et $\dim_G H = r$. Soit un élément x de G ; on peut écrire : $x = \sum_{j=1}^{r} \lambda_j y_j$ et l'on peut développer chaque λ_j (qui est dans G sur F, soit : $\lambda_j = \sum_{i=1}^{q} \gamma_{ij} x_i$ avec $\gamma_{ij} \in F$ et donc $x = \sum_{j=1}^{r} \sum_{i=1}^{q} \gamma_{ij} x_i y_j$; donc la famille $(x_i y_j)$ est génératrice de H sur le corps de base F et elle possède bien qr éléments ; elle est libre car si $\sum_{j=1}^{r} \sum_{i=1}^{q} \gamma_{ij} x_i y_j = 0$ alors chaque $\sum_{i=1}^{q} \gamma_{ij} x_i$ est nul par indépendance des y_j et ceci entraîne la nullité des γ_{ij} par l'indépendance des x_i.

C'est une base et l'on a : $\boxed{\dim_F H = qr = \dim_F G . \dim_G H.}$

Remarque : en théorie des corps, cette dimension s'appelle le degré de l'extension.
b) Lorsque l'on passe d'un corps K_i à une extension quadratique, la dimension sur $\mathbb{Q}$ double d'après la question précédente. Si on a plutôt $K_i = K_{i+1}$ alors la dimension ne change pas. Ainsi, la dimension de K_n, “sommet” d'une pile d'extension quadratiques (strict) vaut 2^n, et s'il y a des corps identiques dans la pile, la dimension du sommet est une puissance de 2, inférieure ou égale à 2^n.
c) Il résulte des études précédentes que si α est constructible, le point de coordonnées $(\alpha, 0)$ l'est, et donc α appartient à un sommet K_n d'une pile d'extensions quadratiques de $\mathbb{Q}$. On peut donc considérer la chaîne de corps : $\mathbb{Q} \subset \mathbb{Q}[\alpha] \subset K_n$; la formule de multiplicativité des dimensions va donner $\deg_{\mathbb{Q}} \alpha \times \dim_{\mathbb{Q}[\alpha]} K_n = 2^p$; ainsi, $\deg_{\mathbb{Q}} \alpha$ divise une puissance de 2, donc est une puissance de 2.



5°) Il s'agit de voir quels sont les nombres de la forme $\cos\dfrac{2\pi}{n}$ qui sont algébriques sur $\mathbb{Q}$ (tous, on l'a vu au I), et quels sont ceux dont le degré est une puissance de 2. Il est à noter que la condition sur le degré n'est pas a priori suffisante, elle est seulement nécessaire.
De fait, seul $\cos\dfrac{2\pi}{5}$ convient à ce point de vue. On sait donc construire les polygones à $3, 4, 6$ côtés (élémentaire), à 5 côtés (on vient de le voir au plan théorique), à 8 et 10 côtés (par bissectrices). les polygones à 7 et 9 côtés ne sont sûrement pas constructibles puisque 3 n'est pas une puissance de 2.
Remarque : Gauss a démontré que pour qu'un polygone régulier à n côtés soit constructible, il suffit que les facteurs primaires de n, de la forme p^r, avec p premier supérieur à 2, soient tels que p soit un nombre de Fermat ($2^{2^n}+1$) et que r soit égal à 1 (à vérifier). Il existe une construction (compliquée, due à Erchinger) du polygone à 17 côtés, car on a

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

Il y a de même une construction du polygone à $2^8+1=257$ côtés, et de même pour $2^{16}+1=65537$. En revanche, $2^{32}+1=4294967297$ n'est pas premier, il est divisible par 641 (selon Euler).
En fin de compte, une liste plus étendue des polygones constructibles serait :

$$3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 25, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80\ldots$$

Section A : Définitions

1°) « Utilisation Commerciale » signifie la distribution ou tout autre moyen de mise à disposition d'un tiers de la documentation.
2°) « Contributeur » signifie une personne ou une entité qui crée ou contribue à la création de modifications.
3°) « Documentation » signifie la documentation originale ou les modifications ou des combinaisons de la documentation originale et les modifications, dans chaque cas, incluant des parties de celles-ci.
4°) « Mécanisme de distribution électronique » signifie un mécanisme communément accepté pour le transfert électronique de données.
5°) « Auteur initial » signifie l'individu ou l'entité qui a été identifié(e) comme étant l'Auteur initial dans la notice obligatoire requise par l'Annexe.
6°) « Œuvre plus importante » signifie une œuvre qui combine de la documentation ou des parties de celle-ci avec de la documentation ou d'autres écrits qui ne sont pas couverts par les conditions de cette licence.
7°) « Licence » signifie ce document.
8°) « Modifications » signifie toute addition, ou suppression, de substance ou de structure d'une documentation originale ou autres modifications précédentes, telles que traduction, abstraction, résumé, ou toute autre forme dans laquelle la documentation originale ou modifications précédentes peut être resaisie, transformée ou adaptée. Une œuvre consistant en des révisions éditoriales, annotations, élaborations, et autres modifications qui, en tant qu'œuvre entière représente une œuvre de l'esprit original, est considérée comme étant une modification. Par exemple, lorsque la documentation est distribuée sous forme d'une série de documents, une modification est comprise comme étant :
A. Toute addition à, ou suppression de, contenu de la documentation originale ou des modifications précédentes.
B. Toute nouvelle documentation qui comporte toute partie de la documentation originale ou modifications précédentes.
9°) « Documentation originale » signifie de la documentation décrite comme étant la documentation originale dans la notice obligatoire requise par l'Annexe, et qui, au moment de sa distribution selon les conditions de cette licence ne constitue pas encore de la documentation couverte par cette licence.
10°) « Forme éditable » signifie la forme préférée de la documentation pour y effectuer des modifications. La documentation peut être sous forme électronique, compressée, ou sous forme d'archive, à condition que le logiciel de décompression ou de désarchivage soit largement disponible de manière gratuite.
11°) « Vous » (ou « Votre ») signifie un individu ou une entité juridique qui exerce des droits conformément à, et en respectant, toutes les conditions de cette Licence ou une version future de cette licence telle que publiée selon la Section D1 (« Versions de la Licence »). Pour des entités juridiques, « vous » couvre également toute entité qui contrôle, ou est contrôlée par, ou qui est sous contrôle commun avec vous. Pour les besoins de la présente définition, « contrôle » signifie
(a) le pouvoir, direct ou indirect, de diriger ou gérer une telle entité, que ce soit de manière contractuelle ou par tout autre moyen, ou
(b) la propriété de plus de cinquante pour cent (50%) des actions libérées ou de la propriété réelle d'une telle entité.

Section B : CONCESSIONS DE LICENCES

1°) Concession de Licence de l'Auteur Initial.
L'Auteur Initial vous concède, par la présente, une licence non-exclusive mondiale, sans redevances, d'utiliser, reproduire, préparer des modifications, compiler, représenter publiquement, afficher publiquement, faire démonstration, commercialiser, divulguer et distribuer la documentation sous toutes formes, sur tous supports ou via tout Mécanisme de Distribution Electronique ou autres méthodes connues aujourd'hui ou à découvrir à l'avenir, ainsi que le droit de concéder des sous-licences les droits énumérés précédemment à des tiers, à travers des systèmes multiples de sous-licences, selon les conditions de cette Licence.
Les droits de licence concédés dans la Section B1 (« Concession de Licence de l'Auteur Initial ») deviennent effectifs à la première date de distribution, par l'Auteur Initial de la documentation originale selon les conditions de cette Licence.
2°) Concession de Licence du Contributeur.
Chaque Contributeur vous concède, par la présente, une licence non-exclusive mondiale, sans redevances, d'utiliser, reproduire, préparer des modifications, compiler, représenter publiquement, afficher publiquement, faire démonstration, commercialiser, divulguer et distribuer la documentation sous toutes formes, sur tous supports ou via tout Mécanisme de Distribution Electronique ou autres méthodes connues aujourd'hui ou à découvrir à l'avenir, ainsi que le droit de concéder des sous-licences les droits énumérés précédemment à des tiers, à travers des systèmes multiples de sous-licences, selon les conditions de cette Licence.
Les droits de licence concédés dans cette Section B2 (« Concession de Licence du Contributeur ») deviennent effectifs à la première date que le Contributeur fait, pour la première fois, une Utilisation Commerciale la documentation.

Section C : OBLIGATIONS DE DISTRIBUTION

1°) Application de la licence.
Les modifications que vous créez ou auxquelles vous contribuez sont couvertes par cette licence, y compris sans limitation la Section B2 (« Concession de licence du Contributeur »). La documentation peut être distribuée seulement selon les conditions de cette licence ou toute version future publiée selon la Section D1 (« Versions de la licence »), et Vous devez intégrer une copie de cette licence dans chaque copie de la documentation que Vous distribuez. Vous ne pouvez offrir ou imposer des conditions qui modifient ou restreignent la version applicable de cette licence ou des droits concédés selon celle-ci. Toutefois, vous pouvez inclure un document additionnel qui offre les droits additionnels décrits à la Section C5 (« Notices nécessaires »).
2°) Disponibilité de la documentation.
Toute modification que Vous créez ou à laquelle Vous contribuez doit être disponible publiquement dans une Forme Éditable selon les conditions de cette Licence à travers un support tangible ou un Mécanisme de Distribution Électronique accepté.
3°) Description des modifications.
Toute documentation à laquelle vous contribuez doit identifier les modifications que vous avez effectuées dans la création du Document, ainsi que la date de telles modifications. Vous devez inclure une déclaration facilement visible indiquant que la modification est dérivée, directement ou indirectement de la documentation originale fournie par l'Auteur Initial et inclure le nom de l'Auteur Initial dans la documentation ou via un lien électronique qui décrit l'origine ou la propriété de la documentation. La documentation modifiée peut être créée par un programme électronique qui suit automatiquement les changements dans la documentation, et de tels changements doivent pouvoir être disponibles pour le public pendant au moins 5 ans après la première distribution de la documentation .
4°) Propriété Intellectuelle.
Le Contributeur garantit que celui-ci croit que ses modifications sont des créations originales du Contributeur, et/ou que le Contributeur détient des droits suffisants lui permettant de concéder les droits indiqués dans cette Licence.
5°) Notices nécessaires.
Vous devez reproduire la notice figurant dans l'Annexe dans chaque fichier de documentation. S'il n'est pas possible d'inclure une telle notice dans un fichier de documentation particulier, du fait de la structure du fichier, vous devez alors inclure une telle notice dans un endroit (tel qu'un répertoire) où un lecteur serait capable de chercher une telle notice, par exemple, via un hyperlien dans chaque fichier de la documentation qui renverra le lecteur vers une page qui décrit l'origine et la propriété de l'œuvre. Si vous avez créé une ou plusieurs modification(s) vous pouvez ajouter votre propre nom, en tant que Contributeur, à la notice décrite en Annexe.
Vous devez également reproduire cette licence dans tout fichier de documentation (ou mettre un hyperlien dans chaque fichier de la documentation) à l'endroit où vous expliquez les droits d'utilisateur ou de propriété.
Vous pouvez offrir à la vente, et faire payer, des services de garantie, soutien, indemnité ou responsabilité civile vis-à-vis d'un ou de plusieurs récipiendaires de la documentation. Toutefois, vous ne pouvez faire ceci que sous votre propre responsabilité, et non pas sous la responsabilité de l'Auteur Initial ni un quelconque Contributeur. Vous devez faire clairement apparaitre que toute garantie, soutien, indemnité ou responsabilité que vous offrez, est faite uniquement par vos soins, et vous marquez par la présente votre accord de dédommager l'Auteur Initial ainsi que chaque Contributeur par rapport à toute demande en garantie envers laquelle l'Auteur Initial ou tout Contributeur pourrait être appelé du fait des services de garantie, soutien, indemnité ou de responsabilité civile que vous offrez.
6°) Œuvre plus importante.
Vous pouvez créer une œuvre plus importante en combinant la documentation avec d'autres documents non couverts par la présente Licence et ainsi distribuer l'œuvre plus importante sous la forme d'un seul produit. Dans ce cas, vous devez vous assurer que les conditions de cette licence soient respectées pour la documentation.

Section D : Champ d'application de la licence

Cette Licence s'applique à la documentation à laquelle l'Auteur Initial a joint cette Licence et la notice qui apparait en Annexe.

Section E : VERSIONS DE LA LICENCE

1°) Nouvelles Versions.
L'Auteur Initial peut publier des versions révisées et/ou nouvelles de la Licence de temps à autre.
2°) Effets des nouvelles versions.
Si la documentation a été publiée selon les conditions d'une version particulière de la licence, vous pouvez continuer à l'utiliser selon les conditions de cette version. Vous pouvez également décider d'utiliser une telle documentation selon les conditions de toute version ultérieure de la licence publiée par Robert Cabane. Personne d'autre que Robert Cabane n'a le droit de modifier les conditions de cette licence. Le fait de fournir le nom de l'auteur initial, la documentation originale ou le contributeur dans la notice décrite dans l'Annexe ne sera pas considéré comme une modification de cette Licence.